

# COMPUTERS & LAW

Journal for the Australian and New Zealand Societies  
for Computers and the Law

Editors: Lesley Sutton and Nicole Wellington  
Number: 43

ISSN 08117225  
March 2001

## Preparing for the new privacy legislation\*

*Tim Dixon, Baker & McKenzie*

Tim Dixon specialises in privacy law as part of the global privacy group at Baker & McKenzie. He chairs the Australian Privacy Foundation and has over ten years' experience working on privacy issues and was a member of the committees established by the Privacy Commissioner and the Commonwealth Attorney-General's Department to work on the National Privacy Principles and the amendments to the Privacy Act. (tim.dixon@bakernet.com)

The arrival of private sector privacy legislation in Australia in 2001 underlines how privacy has emerged as a major business issue. Businesses are grappling with rising customer concerns, a changing regulatory environment, the development of industry codes, and the risk of a public backlash against technologies that raise customer privacy concerns. The growth of e-commerce in particular has raised the profile of privacy issues, and has been a major factor behind the Government's decision to extend the *Privacy Act 1988* to the private sector.

Managing privacy issues often involves balancing competing

interests. On the one hand, businesses have a strong imperative to collect and use personal information. Customer information is critical to e-commerce, and the more that businesses "know" their customers, and know how customers respond to different aspects of their products, the better they are able to target customers with products tailored to their specific interests. This is especially the case in the context of e-commerce companies whose business valuations are based in part on their range and depth of customer relationships.

On the other hand, customers want to retain control of their personal information – a lesson which some

high-profile internet brands have learnt at some expense. Customers are increasingly hostile towards businesses which collect their personal data without their consent, or are not open about how they use this information. In this environment, managing privacy issues effectively can avoid unnecessary risk and help build stronger customer relationships.

Few people would have predicted how sharply the privacy issue has come into focus in recent years. In the early 1990s, privacy was seen largely as a slightly obscure civil liberties issue. But with the technological developments of the internet, payment system encryption, biometrics and


*Continues page 3*



### ***In this issue:***

Preparing for the new privacy legislation .....	1
by <i>Tim Dixon</i>	
From the Editors' Desk .....	2
Canada's New Privacy Law: A Powerful Response to an Important Issue .....	14
by <i>Peter Mantas</i>	
Model Contact Clauses.....	17
by <i>LinkLaters &amp; Alliance News</i>	

Web Bugs and Internet Advertising .....	17
By <i>Kaman Tsoi</i>	
Privacy Online – naked in cyberspace .....	21
by <i>Kimberley Heitman</i>	
Copyright protection of computer programs in Australia .....	24
By <i>Rod Evenden</i>	

 Continued from page 1

data mining, combined with the shift in marketing practices and towards individual customer relationship management, privacy has become a major commercial issue. Privacy has become a political football, a regular news story and a potential risk to company reputations. Industry organisations in many areas have established their own privacy rules which aim to give customers confidence about how their personal information will be handled. Major industry groups are supporting this push. Surveys have recorded unprecedented levels of concerns about privacy issues, which have even been traced back to specific costs. These developments suggest that the right of individuals to control their personal information will be one of the defining social issues in the information age.

The development of privacy

legislation in Australia is part of a global trend to protect personal information and legislate fair information practices. Most advanced countries now have legislation in place which covers the handling of personal information and extends to internet transactions. Australia, like the United States, has lagged behind this trend until now with many countries now implementing second or third generation privacy laws.

**1. Privacy and the e-commerce agenda**

The growing attention to privacy concerns reflects the impact of extensive technological change. The information explosion has made it possible to collect detailed information on customer purchasing patterns, to profile customers and to use data mining to build greater intelligence into business strategies.

While this has offered great convenience to customers, it is also prompting a backlash. Survey research in recent years has tracked rising concerns that consumers are losing control of their personal information. While privacy concerns a decade ago were mainly focused on government collection and use of information, in recent years public concerns have shifted towards the use of personal information in the private sector.

Privacy concerns are now recognised as being more than just a concern for a small proportion of technophobic customers. Unease with the collection and use of personal information is now a significant factor which has held back e-commerce, with consumers reluctant to risk losing control of their personal information despite the convenience offered by the online environment. Analysts now



**COMPUTERS AND LAW**

**Editors**

**Lesley Sutton**  
C/- Freehills  
MLC Centre, Martin Place  
Sydney NSW 2000  
Australia  
(DX 361 Sydney)  
[www.freehills.com.au](http://www.freehills.com.au)  
Tel: +61 2 9225 5169  
Fax: +61 2 9322 4000  
Email: [lesley\\_sutton@freehills.com.au](mailto:lesley_sutton@freehills.com.au)

**Nicole Wellington**  
C/- Freehills  
MLC Centre, Martin Place  
Sydney NSW 2000  
Australia  
(DX 361 Sydney)  
[www.freehills.com.au](http://www.freehills.com.au)  
Tel: +61 2 9225 5229  
Fax: +61 2 9322 4000  
Email: [Nicole\\_Wellington@freehills.com.au](mailto:Nicole_Wellington@freehills.com.au)

Subscription: \$32.00\* per 4 issues

Advertisements: Inserts \$300.00\*; for advertisement within the journal (half page)

Rates and information will be provided by the Editors on request.  
Articles, news items, books for review and other items of interest may be sent to the Editors.

*\*Please see back cover for GST details.*

estimate that billions of dollars worth of e-commerce transactions are being lost because of consumer distrust in current privacy arrangements – as much as \$US2.8bn in the United States in 1999, and rising to \$US18bn by 2002, according to Forrester Research. This research has given impetus to regulatory initiatives in the US and elsewhere.

### 2. Consumer attitudes

Consumer research in Australia and throughout the industrialised world indicates that individuals have serious concerns about their privacy and their sense of losing control of their personal information. A major research project launched by the Federal Privacy Commissioner should provide a deeper insight into how Australians think about privacy issues when it is released around mid-2001.

Existing Australian research reflects similar trends to surveys published in the US, which show a constantly rising trend of privacy concerns. Alan Westin, a veteran US privacy expert who has conducted 26 national privacy attitudes surveys since 1978, notes that privacy concerns have been on a trend increase from a base level of around 72% in the early 1970s. A cross-country survey of the US, UK and Germany conducted in 1999 by IBM Global Research found that:<sup>1</sup>

- consumers have the lowest confidence in the privacy practices of companies which sell over the internet (ranging from 10% to 21%);
- over 50% of consumers surveyed in Germany, the United Kingdom and the US had refused to give information on websites because of privacy concerns, and between 32% and 54% had decided not purchase online because of privacy concerns;
- around a quarter of respondents felt that they had been a victim of invasions of their privacy by businesses;
- concern about possible misuse of personal data ranged from 72% (UK) to 94% (US);
- internet users demonstrate a

higher level of 'privacy-assertive behaviour', such as giving false information when asked to register online.

A Harris Interactive poll of 2,810 American adults in August 2000 found that American consumers are more concerned about privacy issues than health care, crime or taxes. Some 56% stated that they are very concerned about the loss of personal privacy, compared with 54% with health care, 53% with crime and 52% with taxes. Consumers were most worried about websites providing personal information to others without their knowledge (64%) and websites collecting information about them without their knowledge (59%). 65% stated that if a website does not have a privacy policy they will not provide their personal information.

A Business Week/Harris poll in March 2000 showed record levels of privacy concerns for this long-running survey<sup>2</sup>. The survey of over 1000 adults showed:

- out of the 45% of people who have purchased online, 78% said they were concerned about the company they buy from sending them spam (41% very concerned);
- out of the 55% of people who have not purchased online, 94% said they were concerned about the company they buy from sending them spam (63% very concerned), suggesting that privacy attitudes are having a significant effect on consumer behaviour;
- privacy concerns ranked higher than concerns about credit card security (70% of online buyers, and 87% of non-online buyers recorded this concern);
- 37% said they were comfortable with anonymous tracking of website use, but 63% were not;
- 10% were happy with browsing habits and shopping patterns being merged, 89% were against (including 68% 'not at all comfortable');
- 92% did not want sharing of their

personal information (and 7% were comfortable with it);

- 55% of web users had noticed privacy policies, of whom 77% read them – 35% said 'always';
- display of a privacy notice was 'absolutely essential' to 35%, 'very important' to 40% and 'somewhat important' to 21%; only 3% said it was 'not important';
- around 70% said they would use the internet, register personal information or purchase more often if there were explicit guarantees about the use of their personal information;
- consistently around 80% of people wanted an opt-in arrangement for information collection, and 88% wanted to give consent before any sharing of their personal information.

A US survey by Yankelovich Partners released in August 2000 underlined similar concerns. The survey covered 1,173 people and found that:

- 90% of people said that protection of the privacy of their personal information is the most important issue to them when shopping online;
- 79% said that they sometimes left websites which required personal information before they proceeded to look at the content of the site.

Similarly, a survey of 4,523 consumers by NFO Interactive in August 1999 showed that more than 3 out of every 4 consumers who browse but do not buy, indicate that they would be more likely to buy if they were assured that their privacy would be respected. The UCLA Internet Report in October 2000 reported that on the basis of its American survey, part of a global survey, privacy concerns were the single biggest reason why people do not buy online.

These concerns are behind the widespread adoption of comprehensive privacy and data protection legislation in developed countries over the past decade, which are discussed later in this paper. The

European Union has adopted the highest standard, with a privacy Directive which requires detailed compliance from companies handling personal information. Other countries, such as Hong Kong, Canada, New Zealand and Taiwan have implemented comprehensive regimes, with differing levels of flexibility. The United States has attempted to rely more on a sectoral and self-regulatory approach, but this is changing.

The global regulatory patchwork creates challenges for e-commerce which by its nature involves cross-border alliances and transactions. Some businesses are adopting the approach of jumping to the highest bar, the European Union Directive, hoping that this will be adequate for other jurisdictions. Others adapt their policies to local requirements and do not aim for a consistent global strategy. Many have an ad hoc approach which only deal with privacy issues when confronted by customer complaints, negative publicity or because of immediate legal requirements.

The challenge for business organisations is to recognise that privacy is a strategic issue which goes beyond the scope of mere legal compliance. For example:

- protecting personal information is an important element of the trust relationship which businesses want to develop with customers.
- privacy is recognised as a threshold issue for consumer take-up of e-commerce, and is especially important for new products which involve the collection and use of large amounts of personal information, or particularly sensitive information such as health or financial records;
- providing consumers with the widest range of choice in relation to their personal information is an element of quality of service;
- privacy and security features are an important part of risk management strategies, because a negative privacy experience can have a substantial impact on

public perceptions of an organisation's trustworthiness;

- several industry associations have adopted codes of practice which include privacy standards, and which are binding on their members.

### 3. Personal information in an e-commerce environment

Changing business practices have greatly increased the scope for collecting personal information. This reflects the explosion of information gathering, processing and storage in recent years. For example, telecommunications providers know the date, time, length, call number and destination of telephone calls. Pay TV services can know the viewing interests of subscribers. Internet portals can know the interests of users from how users navigate their website. With the development of interactive TV and pay-per-view services, it may also include a detailed history of a household's viewing patterns. Online financial services aggregators and bill management services can also collect a vast amount of highly sensitive information which gives a wide-ranging view of a person's finances.

While businesses were already able to collect a substantial amount of personal information on their customers before the arrival of online transactions, e-commerce creates a much larger and richer store of personal information because very few online transactions are anonymous. There are also far more points of collection of information:

- online registration systems allow businesses to collect contact details and general demographic information;
- clickstream data, collected through cookies, can identify the specific interests of individuals as well as giving companies information about how customers respond to the content of their website;
- email allows customers to communicate with businesses with minimal time or effort; and
- businesses can track a complete

history of customer purchases.

The online environment allows businesses to build individual customer profiles in a way that for most businesses was simply not practicable across a wide customer base in the past. The information gathered from these profiles can be an enormously valuable resource for strategic development as well as for marketing and building customer relationships.

The online environment has also fostered the growth of joint ventures and alliance relationships, where businesses are able to leverage off each other's strengths. A significant online customer base is a highly valuable commercial asset for companies which are entering into joint ventures. In some cases, joint ventures allow companies to access the personal information held by partners and to expand their records as a result. But joint ventures can also contain risks if there is a leakage of customer information to other parties without the consent of those customers.

### 4. The privacy minefield

The risk of adverse media publicity has now become a major reason for businesses to review and change their privacy practices, after an unprecedented year of privacy debacles in 2000. Several high-profile businesses have had their reputations tarnished by lax, inadequate and in some cases illegal information practices. Despite the fact that for several years surveys have highlighted the importance of privacy to consumers, it is only more recently with far greater media coverage of privacy issues that privacy has been recognised as an issue which can significantly harm the public reputation of businesses.

In some respects, it is not surprising that increasing public attention on privacy issues is likely to expose some organisations for bad information practices. Survey research has indicated that many organisations do not have clearly developed or well implemented privacy policies; and while online privacy practices are improving, they fall well short of any

## Preparing for the new privacy legislation

well-accepted privacy benchmark. Even in sectors where a substantial amount of personal information is collected such as online recruitment services, many websites still do not have privacy policies. Among those that have a policy, many do not have adequate privacy standards.

As the spotlight on internet practices has intensified in recent years, a growing list of companies have come under attack for careless, unethical or even deceptive information practices. The public reputations of businesses can be damaged by:

- bad information collection practices, such as collecting unnecessary information;
- failing to explain how personal information will be used (and broadly, failing to develop a privacy policy);
- passing on personal information to other companies without the consent of the person;
- failing to implement the privacy policy;
- security breaches, including unauthorised access to personal information, unintended disclosure, and problems with credit card numbers;
- making mistakes, such as sending the wrong personal information to individuals or recording mistaken information, and
- denying people anonymity, such as in their usage of a website.

These risks are illustrated by some of the privacy stories which hit the news during 2000.

(a) Real Networks: Failing to disclose information practices

2000 began with online software distributor **Real Networks** still smarting from a blitz of negative publicity after the New York Times revealed that it was collecting information about the musical tastes of 13.5m Real product users without their knowledge. Real Jukebox, software downloaded through the Real Networks site, was scanning users' hard drives and transmitting

information about their musical interests and music player back to Real Networks. This information was then added to pre-existing customer profile information.

(b) DoubleClick: Customer profiling without consent

In perhaps the best-known incident of 2000, online advertising agency **DoubleClick** came under seige from public outrage for its plans to combine and sell online and offline customers personal information. DoubleClick is the leading online advertiser, with revenues which had grown from \$9m in 1995 to \$258m in 1999. By the end of 1999 DoubleClick was serving 30 billion targeted ads per month, and serving ads to around 12,000 websites. In late 1999, DoubleClick began combining and cross referencing personal information from the web browsing habits of users with the database of a direct marketing firm, Abacus, which it had recently acquired. DoubleClick planned to match home address, name and purchasing habits to individuals' web Usage patterns. Following extensive publicity, a consumer backlash, legal action by the Michigan State Attorney-General, an FTC investigation and a drop of one third in its share price, DoubleClick suspended its matching practices in March 2000. Estimates of the cost to DoubleClick of the incident – which occurred at the time of its second capital raising – range as high as \$2.2 billion.

(c) Toysmart – selling a bankrupt business's database

American toy e-tailer **Toysmart** drew criticism when it announced that it intended to sell off its customer database after the company filed for bankruptcy on May 19. The decision to sell off the 250,000 customer records contradicted an express promise on Toysmart's web site never to sell customer information. This reversal in policy prompted the intervention of the Federal Trade Commissioner (FTC) who sued Toysmart for engaging in deceptive conduct. 42 states also sought a court injunction from the Federal Court to prevent the sale taking place for violations of their individual consumer

protection schemes. The FTC eventually came to an agreement with the company that precluded the sale of the database as a separate asset, such that Toysmart could only sell the customer database as part of the sale of the whole web site. No company came forward to buy Toysmart, and in early January 2001 Toysmart's majority owner, Disney, paid \$50,000 to destroy the database.

(d) Amazon – Revising a privacy policy

Amazon.com created a storm of protest when it informed customers that it was revising its privacy policy in light of the confusion about the capacity of businesses to sell their databases after the Toysmart.com debacle. The revisions to Amazon's policy stated that the 23 million strong customer database is an asset of the business which may be sold to a third party in the future, without obtaining any further consent from customers. Amazon's changes provoked widespread criticism and several complaints have been filed against Amazon's subsidiaries in Europe for breaching local European privacy standards.

(e) Toysrus.com – Failing to inform consumer of third party use

The toy store e-tail industry was rocked by a further privacy debacle in August 2000 when it was revealed that **Toysrus.com**, the e-commerce web site of the **Toys R Us** chain, was outsourcing data analysis of its consumer database to a third party company, **Coremetrics**, which was then retaining and using the data for its own data analysis purposes. The company's privacy policy made no mention of the outsourcing relationship, which involved the provision of customers personal details including names, postal and email addresses, and phone numbers to Coremetrics. Toys R Us had reserved the right to gather and analyse customer information in its privacy policy, however its failure to disclose the fact that this analysis would be done by another company (which retained the data after analysis) prompted numerous complaints. Two separate class actions were launched against Toys R Us and Coremetrics,

forcing the companies to terminate their business relationship in the wake of overwhelming negative publicity.

(f) Security breaches

Stories of website security breaches which placed customer information at risk became a familiar story during 2000.

- The year began with online music seller **CD Universe** losing more than 300,000 credit cards to a Russian hacker. Credit card cleaning house **Creditcards.com** lost another 55,000 records and in December it was reported that the hackers had broken into the **Egghead** website, potentially gaining access to 3.7 million customer profiles. The company later reported that investigations indicated that the hackers had not gained access to the customer records.
- At the year's end, a hacker broke into the customer database of **GlobalCentral.com**, a Wyoming internet service provider, and sent information on customers including their credit card number, bank account numbers, address, telephone number and terms of their contract with GlobalCentral. The hacker was reportedly motivated by opposition to GlobalCentral's support of a conservative family values organisation.
- Furniture retailer **Ikea** attracted attention when it was revealed that its customer database, containing names, phone numbers and postal and email addresses, was publicly accessible on the web for over two days in early September 2000. The company claimed that the security breach was caused by a hacker, a claim disputed by experts who cited the lack of adequate authentication or firewall software as a contributing factor. The incident was Ikea's second privacy slip-up that year, with the company drawing criticism in March for adopting a spam-based advertising strategy. The company had offered a \$75 discount coupon to any customer who emailed a promotional e-card

to ten of their friends. The scheme generated 37,000 emails within one week before Ikea stopped the promotion in response to severe public criticism.

- On 7 July 2000, a customer of British power utility, **Powergen**, while attempting to pay a bill online, managed to accidentally uncover the unencrypted, publicly accessible credit card numbers and payment and personal details of 7,000 Powergen customers.
- In April 2000, web search engines revealed pages containing the personal registration of some 35,000 members of the **adiamondisforever.com** website, a site which gives information about diamonds and which is sponsored by De Beer's.
- Similarly, a computing error on the **Amazon.com** website resulted in the email address of Amazon members being disclosed on an affiliate partner's website in September 2000.

(g) Australian Taxation Office: Failing to identify a major privacy issue

Privacy issues emerged as a significant problem during the implementation of major tax reforms in Australia in mid-2000. Central to the business tax reforms was the need to obtain an Australian Business Number (ABN) for business to business dealings. Over 3 million applications were received during its first months of operation, although Australian Bureau of Statistics figures indicate that there are only 1.1m businesses in Australia – suggesting most ABNs were for individuals. But the ATO had not taken into account the extent to which individuals would obtain ABNs, and the fact that ABN records would contain a substantial amount of personal information.

Legislation relating to the ABN established a publicly available Australian Business Register, including information on the holders of ABN drawn from the ABN registration forms and, in addition the Tax Office was making available (at a charge of \$20) records of registration-related information. Although the

ABN registration booklet mentioned that some ABN information would be publicly available, the details of this availability were not clear and applicants were not informed of this on the pages where they entered information. After a substantial public reaction, and intervention by the Privacy Commissioner, the Treasurer agreed to legislative amendments and the Tax Office agreed to limit the amount of information available publicly, and give individuals the option of limiting disclosure of their information if this disclosure could present a danger to them.

Privacy concerns were raised in Australia when a hacker accessed the business and bank account details of up to 27,000 businesses in Australia who were accredited suppliers of GST information and assistance packages to businesses through the **GST Start-up Assistance Office**. The 'hacker' reportedly obtained the information without actually hacking the site, as the information was provided on an ordinary page accessible through a URL on the site (the web address of which had not been disclosed). He then emailed 17,000 of the businesses to inform them of the security breach.

(h) Other legal action

In other incidents, Auction site **ReverseAuction** agreed to a settlement with the FTC in January 2000, agreeing to cease from engaging in unlawful practices including collecting personal information of eBay users and deceptive spamming. Other legal action on privacy grounds was also launched against **Amazon.com** (through its subsidiary Alexa Internet, accused of sending personal information to Amazon.com without consent), and a class action suit was filed in Texas against Yahoo! on the basis of a Texan anti-stalking law, arguing that cookies are the cyberspace equivalent of stalking.

**5. The global context of privacy laws**

The extension of Australian privacy legislation is occurring in the context of a rapidly changing global regulatory environment, where privacy has emerged as a major issue in the legal context of e-commerce.

The global nature of information flows raise complex privacy issues because of the potential for personal information to flow from jurisdictions where personal information is subject to privacy regulation, to other jurisdictions where there is little or no legal protection of personal information. This has been an especially controversial issue in recent years, with the European Union's privacy Directive restricting the flows of personal information to countries which do not have an "adequate" level of protection. This restriction has resulted in lengthy negotiations with the United States, which saw this requirement as a restriction on the development of e-commerce, while the EU argued that the US was neglecting a fundamental human right. After several years of meetings, the EU and the US concluded the "Safe Harbour" agreement which gives some protection to the data of Europeans in the United States, and which came into effect from November 2000.

Depending on the regional context of e-commerce transactions and alliances, it may be necessary to take account of the international context of legal protection for personal information. In simple terms, the two main approaches being adopted around the world to protect privacy are comprehensive privacy legislation or a mix of self-regulation and specific sectoral legislation, the approach adopted by the US.

The push towards legal measures to protect privacy began in industrialised nations in the mid-1970s. In the late 1970s, the Organisation for Economic Cooperation and Development (OECD) assembled a group of experts who developed a set of basic privacy and data protection guidelines. The OECD Guidelines, developed in 1980 was the first significant international agreement on privacy principles. These Guidelines formed the basis of privacy legislation in most industrialised nations in the following decade, incorporating eight principles relating to the collection, use, security and disclosure of personal information. However, the OECD Guidelines did not set out an explicit statement on how these principles may be enforced, even in relation to data held by the public sector. As a result,

countries chose a range of measures to implement the privacy principles.

The most significant privacy legislation in the past decade was the **European Union Directive on data protection**, which came into force in October 1998 and is implemented through national legislation individually in EU member states. It establishes comprehensive protection of personal information held by the public and private sectors, whether held electronically, manually or in any other forms. The EU Directive has become the international benchmark for privacy protection - not least because countries without what the Directive describes as an "adequate" level of data protection, will be excluded from personal information flows. An important consideration for Australia is that it would not currently meet these standards. The EU Directive has been a significant factor in countries such as Hong Kong and Canada implementing privacy legislation.

Closest to home, the **New Zealand Privacy Act 1993** established an Office of the Privacy Commissioner who has powers to enforce the Information Privacy Principles contained in the Act in respect of the public and private sectors. The Commissioner is also able to issue Codes, which vary the application of the IPPs for a practice, company, technology or industry. The extension of Australia's *Privacy Act 1988* brings Australia closer to the NZ position, although the Australian legislation is, on several points of comparison, weaker than New Zealand's.

The alternative to the legislated approach is relying more heavily on **self-regulation**, which has been favoured in the United States.

### 6. The United States

The regulatory environment of the United States is particularly influential for e-commerce practices, given the US dominance whether measured by usage, sites, brand names or revenue. In this area, there have been significant developments in the past two years, which appear to be leading to internet privacy legislation.

### 6.1 The Federal Trade Commission

After two years of monitoring the effectiveness of self-regulation, the Federal Trade Commission (FTC) concluded in May 2000 that self regulation had failed to provide adequate privacy protection. While it indicated that significant progress has been made towards the development of industry self regulation, it also noted that coverage of privacy safeguards is still inadequate and that legislation has become necessary. The FTC recommended to Congress that legislation be developed to protect personal information online in its report *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress*.

The FTC's third survey of the practices of popular websites was conducted in early 2000, with the aim of checking their compliance with privacy principles. The survey noted at the time that some 90 million Americans were using the internet on a regular basis, and that over 60 million shopped online in the third quarter of 1999, with just over half internet users having actually bought an item online. An estimated \$20-\$33bn of online retail sales were made in 1999, and internet advertising was worth \$4.6bn. The survey noted recent research showing that 67% of consumers were very concerned about the misuse of their personal information online, and a total of 92% had some level of concern.

The survey reviewed a random sample of 335 websites and a group of 91 of the busiest 100 websites. The survey confirmed that most sites collect personal information - 97% of the random websites and 99% of the busiest websites - and that 88% and 100% respectively made some kind of statement about their privacy practices.

However, the survey reported that most of the privacy policies failed to meet the standards of the four main criteria of fair information practices - notice, choice, access and security. Only 20% of the sites implement, in part at least, the four fair information



practices. While this represents an improvement on the previous study in early 1999, the improvement was only marginal and it was not enough to convince the FTC that self-regulation is working effectively. Even on the two criteria of notice and choice, only 41% and 60% of the two groups of websites met the standards of the fair information principles. The report also noted that privacy seal programs applied to 8% of the random sample of websites and 45% of the popular websites.

The report concluded that:

"Because self-regulatory initiatives to date fall far short of broad-based implementation of effective self-regulatory programs, the Commission has concluded that such efforts alone cannot ensure that the online marketplace as a whole will emulate the standards adopted by industry leaders. While there will continue to be a major role for industry self-regulation in the future, the Commission recommends that Congress enact legislation that, in conjunction with continuing self-regulatory programs, will ensure adequate protection of consumer privacy online."

Robert Pitofsky, Federal Trade Commission chairman, stated in March 2000 that:

- surveys indicated that 61% of internet users do not purchase on-line because of fears about the security of their personal information;
- 90% of those who buy goods on-line still express concerns about doing so;
- the FTC's hotline for logging identity fraud was logging 400 calls per week, and Pitofsky expects this to reach 200,000 per year. A similar hotline relating to misuse of social security numbers reached 39,000 calls in 1999.

Public attitudes towards privacy issues in the United States have also hardened. The annual Business Week/Harris Poll on American privacy attitudes in March 2000

recorded the highest ever concerns about privacy issues. Asked about how governments should respond on the privacy issue, 67% stated a preference for the strongest option, that is for the government immediately implementing laws for how information should be collected and used on the internet.

### 6.2 Moves to legislate privacy protection in the US

Forrester Research's report *Privacy Self-Regulation Will Fail*, concluded that legislators and regulators will not wait for self-regulation to work, and that legislation is almost inevitable because business and consumer groups cannot reach common ground on privacy principles. In fact, the Forrester report argues that customer-profile driven e-commerce is inherently in conflict with protecting consumers' privacy. "To avoid regulation, companies must convince the FTC that substantial progress has been made towards fair information principles [but] asking this group to reach consensus is like expecting hospitals, insurers and patients to agree on managed care."

The FTC's recommendation for legislation would cover consumer-oriented commercial websites. In other words, it would be a specific internet privacy measure, rather than the comprehensive data protection legislation adopted by most other advanced nations. It would therefore continue the blend of sectoral legislation and self-regulation which has been adopted by the US in recent years. The FTC's legislation would require that these websites comply with the four widely-accepted fair information practices of:

- Notice – in which websites would need to give clear, conspicuous notice of their information practices including information about what is collected, how it is collected, how it is used, how consumers are given choice, security, any access, whether information is disclosed to third parties and whether third parties collect information off the website.
- Choice – in which websites would

be required to give consumers choices about how their information is used for purposes beyond the original purpose of its collection, including internal and external secondary uses.

- Access – in which websites would give consumers reasonable access to the information which has been collected about consumers, and reasonable opportunity to review information and correct any inaccuracies.
- Security – in which websites would be required to take reasonable steps to protect the security of the information obtained from customers.

These principles are a shortened version of the 1980 OECD principles, and are less extensive than the National Privacy Principles in Australia's Privacy Amendment (Private Sector) Act.

The internet industry in the United States is increasingly recognising the likelihood of privacy legislation. As in Australia, one of the strongest drivers of a national privacy regime in the United States is the concern of business groups to avoid a patchwork of inconsistent state-based privacy laws. New York, California, Maryland, South Carolina, Florida, Wisconsin and other states have been debating broad privacy laws. The American Electronics Association began a push for a uniform national privacy law in 2000, to avoid a "privacy maze".

Meanwhile, Attorneys-General in various states were talking about specific legal rights – in New York, Eliot Spitzer wanting a ban on the sale of web surfer's personal information; in Washington State, Christine Gregoire wanting consumers to be given rights to access and control their personal information, with legal rights to sue; Maryland Governor Parris Glendening wanting to ban spam and protect public register information from misuse.

In some states, individuals – sometimes backed by governments – have begun taking the law into their own hands. Yahoo! faces a creative claim under Texan anti-stalking laws



for its use of cookie technology which according to Dallas lawyer Lawrence J. Friedman allows the organisation "to watch, to spy, to conduct surveillance, to analyse the habits, inclinations, preferences and states" of people who visit its sites "without consent, agreement or permission of the class members". Friedman is claiming \$50bn in economic damages – and despite its inventiveness, if it gets a plaintiff-friendly Texan jury in an environment of frustration over internet privacy the outcome cannot be certain.

Congress had dozens of privacy statutes on its agenda in 2000, and both the President and Vice President gave addresses on privacy issues during the year. None of the Congressional Bills drew widespread agreement, but they foreshadow the likelihood of an eventual agreement on legislation. The proposals range from a general study of privacy issues (the *Privacy Protection Study Commission Act*), to requirements that consumers give explicit, opt-in consent for sharing of data, as well as annual reports on data usage and the right to sue for misuse of data (*Personal Data Privacy Protection Act*). In between, proposals such as the *Online Privacy Protection Act* (with bipartisan sponsorship) and the *Electronic Privacy Bill of Rights Act* require privacy policies on websites, rights to opt-out of disclosure of information to third parties and rights to access personal data.

A working group of Congress members from both houses and both parties was formed in late 2000 with the aim of reaching a consensus on new privacy laws, likely to impose a set of baseline requirements to which all Websites might have to adhere under the working group's compromise legislation. In line with FTC recommendations, the legislation would require that the websites give information about the collection and use of personal information, and visitors to websites would be able to choose either to opt out of the collection of their personal information or to limit the use of the information. The Federal Trade Commission would have oversight of implementation of the law.

By early 2001, 13 privacy Bills had already been introduced into the new Congress, and several from 2000 are expected to be reintroduced. The bipartisan Congressional Privacy Caucus is working towards a privacy Bill that embodies basic privacy principles and may even ban some internet tracking technologies such as web bugs.

### 7. The Privacy Act 1988 and the Privacy Amendment (Private Sector) Act 2000

#### 7.1 Background: Coverage of privacy legislation prior to amendments

Although online developments have heightened privacy concerns, the history of specific legal measures to protect privacy in Australia reaches back into the early 1970s. The first regulatory agency to have responsibility for privacy issues, the New South Wales Privacy Committee, was established in 1975.<sup>4</sup> In 1976 the Australian Law Reform Commission began working on a major national report on privacy, which was released in 1983. The *Privacy Act 1988 (Cth)* was a delayed response to the recommendations of this report, and was initially to be introduced alongside the proposed Australia Card, the national identity card which was abandoned after an extraordinarily negative public reaction.

Prior to the recent amendments, the Privacy Act 1988 was based around a set of 11 Information Privacy Principles, formulated from the 1980 OECD Guidelines, covering issues such as the collection, use, security, disclosure, retention and destruction of personal information. The Privacy Act 1988 had only a limited scope, essentially applying to:

- (a) Commonwealth Government agencies
- (b) the handling of Tax File Numbers (TFNs) by all organisations (a set of mandatory Guidelines which restrict the use of TFNs); and
- (c) the use of credit reporting information in the private sector.

At the state level, governments have

implemented similar legislation with the *Privacy and Personal Information Protection Act 1998 (NSW)* and the *Information Privacy Act 2000 (Vic)*.

In overall terms, personal information collected by the Commonwealth Government and some states was covered by privacy legislation, but these laws had limited impact on the private sector.

Specific statutes also address the use of particular technologies in the private sector; for example, the *Telecommunications Interception Act 1979* and state legislation such as the *Listening Devices Act 1984 (NSW)* and the *Surveillance Devices Act 1999 (Victoria)* prohibit the unauthorised interception and recording of telephone conversations. The *Telecommunications Act 1997* also imposes restrictions on the unauthorised disclosure of personal information related to customers of a telecommunications service provider or an internet service provider.

There is a very limited degree of common law recognition of what might be seen as a right to privacy in special situations. For example, if it is seen that a duty of confidentiality exists between two parties (eg bank and customer or a doctor and patient), then disclosure of information to a third party may be a breach of confidence.

Outside the framework of legislation, some companies and industry organisations have adopted a self-regulating approach to privacy protection:

- individual industries have specific codes of conduct which can govern the practices of members of industry organisations or sectors. For example, the National Privacy Principles are being incorporated into revised versions of the Code of Banking Practice (which already deals with a variety of privacy issues in clause 12), and the Electronic Funds Transfer code of conduct (which already has some specific safeguards such as those relating to the use of cameras at Automated Teller Machines);
- individual industry bodies such as

the Banking Industry Ombudsman and the Telecommunications Industry Ombudsman (TIO) receive and investigate complaints relating to privacy breaches within their industries. In the case of the TIO, membership of the body is compulsory for carriers, carriage service providers and internet service providers. The Australian Direct Marketing Association requires all of its members to comply with privacy obligations in its code, and plans to register this code with the Privacy Commissioner.;

- some individual companies may establish internal guidelines on privacy. For example, Telstra has developed a corporate privacy policy which is subject to an annual external audit, overseen by an independent panel;

7.2 The evolution of the current privacy legislation

The amendments to the Privacy Act 1988, concluded in Parliament in December 2000, are the result of several years of policy debate inside and outside of Parliament. The legislation is based around the National Principles for the Fair Handling of Personal Information (the National Privacy Principles) first developed by the Privacy Commissioner's office in 1997 and 1998. Before its election to government, the Howard Government had promised strong privacy legislation. After switching positions and arguing in favour of a self-regulatory approach to privacy protection in 1997, the Government shifted again back in favour of a "co-regulatory" model combining industry codes and minimum standards. While the model attracted substantial criticisms during its passage through Parliament, from both House and Senate committees, it made its way through the Senate at the end of 2000.

Four main factors prompted the change in the Howard Government's position away from self-regulation:

- the Victorian Government had indicated that it would go ahead with private sector privacy

legislation if the Commonwealth Government failed to legislate. This in turn threatened to contribute to an untidy patchwork of different laws in separate states and industry sectors, and prompted industry groups to press for Commonwealth privacy legislation;

- the European Union's Privacy Directive prohibits trade in personal information with countries which do not have adequate privacy protection (effective from October 1998). Because there are no enforceable privacy safeguards in the private sector, Australia would not meet the test of adequacy, with potentially significant negative implications for the information industries in Australia;
- consumer research has indicated that privacy protection is a pre-requisite for establishing consumer confidence in new technologies.

7.3 Understanding the National Privacy Principles: The life cycle of personal information

In a general sense, privacy legislation seeks to protect individuals from the unfair or unauthorised use of their personal information. These rights can be understood through the 'life-cycle of information': from collection, through to use and disclosure to third parties, and ultimately to the destruction of the information. Privacy laws seek to protect the individual's right to control the use, storage and disclosure of this personal information, subject to other public interests such as law enforcement and the efficiency of public administration. As Professor Alan Westin first defined it, privacy legislation protects the individual's right to "determine for one's self when, how, and to what extent information about one's self is communicated to others."<sup>7</sup> This right "can protect autonomy, dignity, or health and welfare."<sup>6</sup>

The National Privacy Principles (NPPs) set out minimum standards for the handling of personal information. To a large extent these principles

reflect the OECD's *Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data* from 1980. The NPPs differ from the Information Privacy Principles (IPPs) which apply to Commonwealth Government agencies. In the shortest form, they may be summarised in this way:

- **Collection of personal information:** Collection must be necessary for an organisation's activities, information must be collected lawfully and fairly, and as a general principle must be collected with the individual's consent.
- **Use and disclosure of personal information:** As a general principle, information can only be used or disclosed for its original purpose unless the person has consented to its use or disclosure for another purpose. Exemptions apply to initial contact for direct marketing (if consent wasn't practicable originally) and other situations such as when there are issues of law enforcement, public safety or protecting the company from fraud.
- **Accuracy of personal information:** Organisations must take reasonable steps to ensure that they keep personal information accurate, complete and up to date.
- **Security of personal information:** Organisations must take reasonable steps to protect the personal information which they hold from misuse, loss unauthorised access, modification or disclosure.
- **Openness in relation to the organisations practices:** Organisations which collect personal information must be able to document their practices and must make this information available on request.
- **Access and correction rights:** As a general principle, organisations must give individuals access to their personal information and must allow them to correct it or explain something with which they disagree, unless disclosing

this would have an unreasonable impact on someone else's privacy. This principle is subject to exemptions such as if this disclosure would compromise a fraud investigation.

- **Use of government identifiers:** Organisations cannot use a government agency's identifier as its identifier. This would cover items such as drivers' licence numbers, Medicare numbers, a Tax File Number (which in any case is covered by other legislation) or any future identity numbers assigned by a government agency.
- **Anonymity:** Organisations must give people the option of entering into transactions anonymously where it is lawful and practicable. For example, this would apply to travel on a bus, but not to opening a bank account.
- **Restrictions on transborder data flows:** As a general principle, organisations can only transfer the personal information about an individual to a foreign country if they believe that the information will be protected by a law or a contract which upholds privacy principles similar to the NPPs.
- **Special provision for sensitive personal information:** A higher level of privacy protection applies to sensitive personal information, which includes information about a person's health, political or religious beliefs or affiliation, and sexual preference. This information must only be collected with the individual's consent.

These principles reflect in the basic privacy and data protection guidelines developed in the late 1970s by the Organisation for Economic Cooperation and Development (OECD) 7. These Guidelines formed the basis of privacy legislation in most industrialised nations in the following decade, incorporating eight principles relating to the collection, use, security and disclosure of personal information. However, the OECD Guidelines did not set out

requirements as to how these principles may be enforced, even in relation to data held by the public sector. As a result, OECD member countries have chosen a range of differing measures to implement the privacy principles.

### 7.4 Coverage

The NPPs apply to all organisations (other than public sector organisations, which are already covered by the Information Privacy Principles). This includes a body corporate, an unincorporated association, a partnership, a trust or an individual. However, the legislation gives proposed exemptions for:

- (a) **Small Businesses:** A small business is defined as a business with an annual turnover of \$3 million or less, which does not provide a health service or hold health information, which does not provide contractual services to the Commonwealth and does not transfer personal information about an individual to anyone else for any kind of benefit. In other words, small businesses are covered if they are involved in the sale of personal information. This outcome reflects some unique political sensitivities in the Australian political climate relating to small business.
- (b) **The Media:** Acts or practices done by an organisation in the course of journalism will be exempt from the legislation. This provision explicitly aims to strike a balance between the public interest in providing adequate privacy safeguards with the public interest in allowing a free flow of information to the public through the media. The scope of this exemption is especially broad. An organisation can be classified as a media organisation if it is engaged in the provision of information to the public, and its "activities consist of ..... dissemination of ..... material having the character of news, current affairs, information or a documentary". This attracted criticism because of the possibility of it being used as a loophole.

- (c) **Political parties:** Registered political parties will be exempt from the legislation for their activities in connection with an election, a referendum, or other participation in the political process. This was a surprise inclusion in the legislation, as it had never previously been raised during the extensive consultations over the legislation. The Government has argued that it is necessary to give this exemption in order to give effect to the implied constitutional freedom of political speech.

- (d) **Domestic use:** This exemption applies to use of personal information related to personal, family or household affairs relating to personal information.

The Act covers all types of personal information which are not publicly available but, will exclude:

- (a) **Employee records:** Employee records are defined as a record relating to the employment of an employee including engagement, training, disciplining, resignation, termination, terms and conditions, contact details, performance or conduct, remuneration, the union membership, health information and financial affairs. It extends to current and former employers.
- (b) **Personal information already in existence** when the amendments come into operation will have a limited exemption.
- (c) **State government contractors:** The acts and practices of contractors to state and territory governments and agencies in relation to handling personal information under contracts need only to comply with the applicable standards of the state or territory and will otherwise be exempt from the Act.
- (d) **Transfers of personal information between "related bodies corporate"**, as defined under section 50 of the *Corporations Law*. Related bodies corporate are essentially businesses which have a shared controlling interest. This might allow a large organisation with

diverse businesses to pool its personal data collections without the knowledge of its customers. Restrictions still apply to the use and disclosure of this information, but as an example, an organisation which was able to conduct direct marketing to customers seemingly can conduct direct marketing in respect of all of the operations of its related bodies corporate.

The complexity of the exemptions attracted criticism from some industry and consumer groups. The reports from the majority government-member House of Representatives Legal and Constitutional Affairs Committee and the majority Opposition-member Senate Committees recommended substantial changes to restrict the proposed exemptions. However, when the legislation was squeezed through in the closing days of Parliament in December 2000 the exemptions were left intact.

### 7.5 Privacy Codes

By default, the NPPs apply to organisations - that is, unless the organisation is a signatory to a voluntary code which has been approved by the Privacy Commissioner. However, the legislation leaves open the option of industry groups or individual firms developing their own codes of conduct in place of the NPPs. Codes can be developed by any organisation or group, but cannot impose a lower standard or privacy protection than the NPPs. Codes must be approved by the Privacy Commissioner after a process of consultation. The codes are intended to give the legislation maximum flexibility while retaining a consistent standard of privacy protection.

### 7.6 Enforcement

Once in place, an individual who believes that the code has been breached may make a complaint to the organisation concerned. If it is not resolved satisfactorily, they may make a complaint to the Privacy Commissioner, or if an independent adjudicator has been appointed to administer the code, they must make the complaint to that body.

If there is an approved code of conduct in place, the complaint will normally be handled by a code authority, who is established and funded by an industry. In practical terms, this might be the Telecommunications Industry Ombudsman, the Banking Industry Ombudsman or the code authority for the Australian Direct Marketing Association code of conduct. If there is no approved code of conduct in place, the complaint is handled by the Privacy Commissioner.

Breach of the NPPs can result in an order from either a code authority or the Privacy Commissioner to restrain an action, undertake an action, or to give monetary compensation.

A decision by a code authority can be reviewed by the Privacy Commissioner, and the Privacy Commissioner's decision can be reviewed through the process of administrative review.

A decision to give an individual a remedy can be appealed in the Federal Magistrate's Court, and can be enforced through the Court if an organisation has not complied with the remedy.

### 8. Developing a privacy strategy

The best response to the public concerns and changing regulatory environment for privacy issues is to adopt a strategic approach which identifies the importance of privacy issues to an organisation and the specific methods which the organisation intends to use. There are several elements to a privacy strategy, the detail of which will be determined by the nature of the information which is collected and used, the size of the organisation, the extent of the risk to customers' privacy and the reputation of the business. A privacy strategy might include such elements as:

- a clear, detailed website privacy policy;
- opt-in or opt-out consent clauses;
- internal compliance systems, and clear management responsibility;

- conducting an independent audit;
- privacy impact assessments;
- privacy seal programs;
- complaints handling;
- consultation processes;
- outsourcing arrangements;
- the use of technologies to enhance privacy;

It is important to put the contractual and legal context of privacy protection into the broader context of technologies which can play a role in protecting individual privacy. Legal measures are not the only way of providing consumers with protection for their personal information. A small segment of the online community is willing to pay to take privacy protection into its own hands through the use of encryption and other software products which block cookies and preserve online anonymity. These privacy technologies are useful for email, browsing websites and making transactions.

### Conclusion

Privacy has moved from being a relatively obscure civil liberties issue to becoming a critical building block for Australia's information economy. It is also a part of Australia's competitive positioning in the global information economy. The legal protection of personal information reflects public expectations, and for this reason businesses must think of not only how to meet their forthcoming legal obligations, but also to consider whether they handle sensitive personal information and what their customers expect from them. In that sense, privacy should be seen as a strategic challenge and opportunity, and not just a technical issue of legal compliance. In order to build consumer trust, manage information effectively and avoid any privacy landmines, businesses need to ensure that they align their privacy strategy to their broader strategic direction.

- \* Tim Dixon, Baker & McKenzie E-Strategy, Australasia 2000 conference, December 13 2000, tim.dixon@bakernet.com
- 1 Information presented at 21<sup>st</sup> International Conference on Privacy and Data Protection, Hong Kong, 13-15 September 1999
- 2 "Privacy on the Net: A Growing Threat", Business Week, 20 March 2000 (cover story)
- 3 OECD Guidelines covering the protection of privacy and transborder flows of personal data, Paris, 1980
- 4 *Privacy Committee Act 1975 (NSW)*
- 5 Westin, A. *Privacy and Freedom*, New York, 1967, p39, quoted in Goldman, J. "Privacy and individual empowerment in the interactive age", paper presented at the *Visions for Privacy in the 21st Century* conference, Victoria, British Columbia, May 9-11 1996, p26
- 6 Trubow, G. *Protocols for the secondary use of personal information*, unpublished paper, John Marshall Law School Centre for Informatics Law, February 22 1993, p4
- 7 OECD Guidelines covering the protection of privacy and transborder flows of personal data, Paris, 1980

---

## Canada's New Privacy Law: A Powerful Response to an Important Issue

*Peter Mantas, Heenan Blaikie, Canada*

---

Peter Mantas is a technology lawyer in the Ottawa office of the law firm of Heenan Blaikie, one of Canada's largest law firms. He is a guest lecturer at the University of Ottawa Law School and visiting professor at the Universidad del Mayab, Mexico. He is a frequent speaker and writer on numerous technology law issues including the new privacy law in Canada, and advises clients on intellectual property, corporate and litigation matters. He can be reached at pmantas@heenan.ca.

---

On January 1, 2001, a new law regarding the protection of personal information came into force in Canada. The *Personal Information Protection and Electronic Documents Act* (the "Act") was passed by the Canadian federal government to address a wide range of issues affecting the privacy of Canadians. The Act was seen as a necessary response to the growing ability of organizations, particularly through the Internet, to collect and manipulate personal data.

In addition, the Canadian government believed that by passing such a law, electronic commerce in Canada would be enhanced, which was an important goal of the Liberal government and Prime Minister Jean Chretien. Studies presented to the government suggested that there was a perception by the general public that privacy was not respected on the Internet, and that data submitted to websites was routinely exploited for uses unknown and unwanted by web surfers. This led the federal government to conclude that a privacy law would provide users of the Internet in Canada with the confidence to do more, rather than less, business online.

The government was also persuaded to pass the Act for several other reasons. First, the European Union had recently passed a directive which restricted the flow of personal information collected in Europe to countries which did not have a privacy law. Canada saw this both as an obstacle to electronic commerce with Europe, and an opportunity to pick up business from the United States, which did not have acceptable privacy legislation, either in force or impending.

Second, Canadians were increasingly demanding a law to protect their privacy. With the power of the Internet, Canadians became more aware of the ability of organizations to collect, use and disclose information about their person. With this awareness came a growing sense of concern that their individuality was being compromised, that their security and affairs might be adversely affected, and that they would be subjected to annoying material from companies using their personal data for profit.

The Act passed by the Canadian government was broad, novel, and powerful in its enforcement capabilities. Consequently, the Act has been controversial, and it is likely

to be the subject of litigation in the future. In particular, groups that have come to rely upon the free flow of personal information, such as the medical industry, are concerned that their interests will be seriously affected. However, the new law has been well received by many Canadian individuals who believe that privacy, from a human rights perspective, is an important right that ought to be protected.

The Act is divided into two parts. The first part deals with privacy and the second addresses electronic documents. Each part operates independently and this paper will discuss only part one, as this paper is intended to review Canada's new federal privacy law.<sup>2</sup> The Act also incorporates, as a Schedule, the Canadian Standards Association Model Code for the Protection of Personal Information (the "Code"), a private sector initiative which predated the Act.<sup>3</sup> Bringing the Code into the statute was an unusual technique which had the advantage of presenting the rules of the Act in plain language that was already known to the public and had been tried and tested. Unfortunately, simply appending a Schedule, drafted not as a federal statute but as a private sector