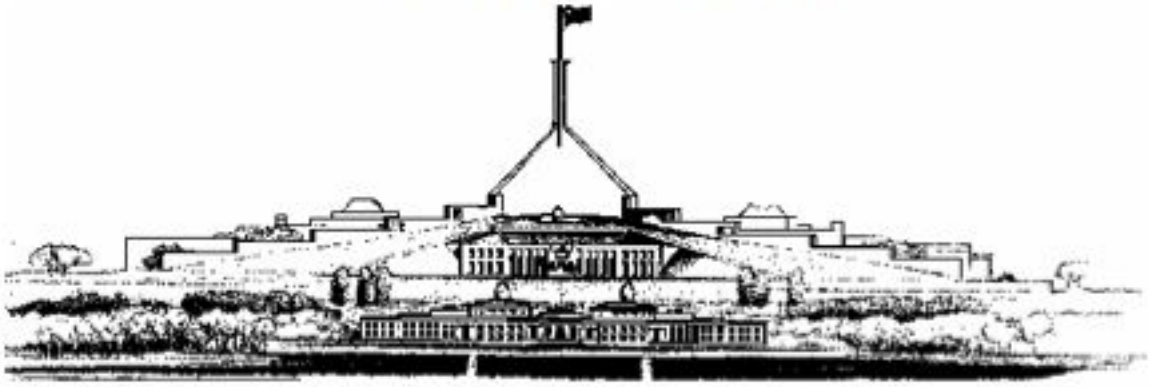
COMMONWEALTH OF AUSTRALIA

PARLIAMENTARY DEBATES



HOUSE OF REPRESENTATIVES

PRIVACY AMENDMENT (PRIVATE SECTOR) BILL 2000

Second Reading

SPEECH

Tuesday, 7 November 2000

BY AUTHORITY OF THE HOUSE OF REPRESENTATIVES

SPEECH

Date	Tuesday, 7 November 2000	**Source**	House
Page	22299	**Proof**	No
Questioner		**Responder**	
Speaker	Pyne, Chris, MP	**Question No.**	

Mr PYNE (Sturt) (5.18 pm)—I rise to speak on the Privacy Amendment (Private Sector) Bill 2000. The social contract that operates in Australia provides that every Australian has a reasonable expectation that their privacy be sacrosanct. We tend to take a very dim view of our individual privacy being compromised. The proliferation of the Internet and e-commerce has challenged our traditional notions of privacy regulation. Statistical and anecdotal evidence suggests that Australians are reluctant to embrace e-commerce until such time that they feel their privacy is sufficiently protected. An excellent article by *Australian Financial Review* correspondent Dorothy Kennedy canvassed many of these themes. A recent report from the Australian Bureau of Statistics shows that 43 per cent of Australian adults accessed the Internet in the 12 months to February 2000 but, by way of contrast, only five per cent purchased products online in the same period.

A report on Internet privacy, published by Australian law firm Freehill Hollingdale and Page, claims that Internet users not only are sceptical about the security of their personal information online but are uncertain about how their information will be used and worried about being inundated with advertising material that they do not want. Clearly consumer behaviour and consumption patterns are being influenced by a lack of consumer confidence in the protection of individual privacy on the Internet. If we can overcome this by introducing more effective privacy provisions, Australian business and Internet businesses will benefit.

There is a precedent for this claim. Late last year, Internet advertising company DoubleClick announced it was acquiring a direct marketing company, Abacus Direct. It was the intention of DoubleClick to link the personal data from Abacus Direct with its own marketing information, obtained by tracking customers' online movements. What DoubleClick had not counted on was the enormous public and media backlash that ensued. In announcing the company's backdown from the plan, DoubleClick's Chief Executive Officer, Kevin O'Connor, explained that he was mistaken to attempt to implement the database in the absence of government and industry privacy standards. In a recently released book entitled *The End of Privacy: How Total Surveillance is Becoming a Reality*, the author, Professor Reg Whittaker, writes about what he terms `dataveillance', which he describes as the new phenomenon of data collection and storage.

This brings us to the bill before the House, the Privacy Amendment (Private Sector) Bill 2000. This bill creates a new benchmark for national standards for the handling of personal information by the private sector. The legislation offers Australians the confidence that information held about them by private sector organisations will be stored, used and disclosed in a fair and appropriate way. Importantly, this bill gives Australians the right to gain access to that information and a right to correct it if it is wrong.

The provisions of this bill deliver market confidence to Australian consumers, the Australian business community and international interests that personal information sent to Australia will be stored safely and handled appropriately. The bill relies on the 1980 OECD Guidelines for the Protection of Privacy and Transborder Flows of Personal Data, which represent a consensus among our major trading partners on the basic principles that should be incorporated into privacy regulation. The measures contained in this bill also implement certain obligations under article 17 of the International Covenant on Civil and Political Rights.

But the cornerstone of this legislation is the National Principles for the Fair Handling of Personal Information. The Privacy Commissioner developed these principles following extensive consultation with business, consumers and other stakeholders. The national principles are a set of guidelines for the collection, holding, use, disclosure and transfer of personal information. When an organisation or industry fails to put a privacy code in operation, the national privacy principles will apply. The national principles also serve as the yardstick for industry codes. The Privacy Commissioner cannot approve a code until he or she is satisfied that it provides at least the same level of protection as the national principles. An important feature of this bill is that it delivers to consumers the right to access information collected on them and to allow individuals to have the information corrected if it is shown to be erroneous. This bill also ensures that mechanisms are in place to deal with consumer complaints and breaches of privacy regulations.

The Australian Competition and Consumer Commission recently reported that 75 per cent of the e-commerce web sites examined by international protection agencies, including the ACCC, had no privacy policy or statement of how consumers' personal details would be handled. There is clearly a void in the e-commerce industry to be filled by corporations that offer their clients privacy protection. The European Union has already attempted to stake its own claim by announcing earlier this year that companies holding data on European citizens must comply with European data privacy laws. However, some commentators believe that the rules put in place by the European Union are unwieldy and unworkable. The provisions of this bill will help establish international consumer confidence in Australian e-commerce web sites and give Australian e-commerce a competitive advantage over its international competition.

But there are already new emerging challenges for government with regard to privacy protection and the private sector. New media, in particular, is spawning a fresh range of problems for government, as legislation throughout the world struggles to keep pace with technology. The emergence of the CrimeNet web site and the proposed `wanted world wide' web site are cases in point. CrimeNet is the self-styled world first Internet based crime information service. With offices in Victoria and Western Australia, the CrimeNet web site catalogues an expanding database of 4,000 to 5,000 Australians who have transgressed the law in the past. The directory of names—which lumps drink-drivers alongside murderers and rapists—is available to curious web viewers at no charge. To inspect more definitive details on each person listed, it costs the viewer $6 for the initial view and $2 for each subsequent search. Although the commencement of the `wanted world wide' service has been delayed by several months, the web site intends to list criminal records as well as bad debtors, child support recovery lists and tenancy related debts.

The emergence of these vigilante and voyeuristic web sites has coincided with the appearance of unwelcome problems for society in terms of privacy concerns and the justice system, with the expectation of more to follow. The foundation of our judicial system is the right to a fair trial and the presumption of innocence until proven guilty. Criminal proceedings are determined on the facts before the court and not on probability based on a past record. The advent of these web sites compromises the integrity of the justice system by allowing jurors to be prejudiced by viewing the criminal history of the accused. If traditional media publish the criminal record of an accused before or during a trial, the proceedings could be aborted and the media outlet cited for contempt of court. Yet here is a web site publishing people's pasts to anyone who has $6. New media outlets such as CrimeNet and `wanted world wide' need to be brought into line with the rules that regulate traditional media to protect the privacy of the individual. The Managing Director of CrimeNet, Mr Ken Schultz, makes the desperate claim that those accessing the web site now need to sign a type of cyber guarantee that they will not misuse the information. This is a superficial, unworkable and facile response. As I understand it, this `cyber guarantee' has yet to be tested in a court of law with regard to contempt of court. But, if it were to pass that test, it still fails dismally to protect the privacy of the named individuals.

The appearance of these web sites also threatens to undermine the criminal rehabilitation process. If you do the crime you have to do the time. But once a person has been punished and freed by the justice system their right to privacy should not be diminished because of past mistakes. They and their families have a right to start again and should not face the threat of community ridicule and discrimination at the hands of Net cowboys. The emergence of these web sites exposes innocent people to the possibility that defamatory material may be mistakenly published about them. In response to this risk, the CrimeNet web site meekly offers:

> We do our best to maintain accurate records. All entries are checked by our Editor. However, if you believe the information relating to any person listed on this site, is inaccurate or incorrect, you may request a correction by sending details together with documentary evidence to—

And then it gives an address. It would be a bit late—the horse will have bolted—if someone's reputation has been slandered by this web site and then they ring up and say, `By the way, it is not true that I am the rapist you were referring to in the CrimeNet web site.' This is simply an exercise in covering your back, and does nothing to protect the privacy of persons who are wrongly named. It is a ham-fisted and ineffective attempt to avoid responsibility for what could cause irreparable damage to an innocent person's character and reputation. CrimeNet's disclaimer will be cold comfort to the unintended victim of their flawed data collection process.

This flawed data collection process also manifests itself in another potential problem for innocent Australians. The web site editors do not compile their databases from official records, but rather from previously published material such as newspapers. So what happens in those instances where an individual is convicted but later acquitted on appeal, or in those circumstances where information in the newspapers is inaccurately reported?

As this genre of web sites evolves it may well lead to the proliferation of more privacy invasive web sites. Think of the next generation of these web sites, which may include databases of people who have experienced marital problems, mental health difficulties and financial troubles. A coordinated response, encompassing a framework of regulations, needs to be developed to prevent these sites from operating in a way that may damage the reputation of innocent people, potentially prejudice the right to a fair trial and invade the privacy of fellow Australians.

Other enterprises and services that may be offered on the Internet include the storage of individuals' health records and information. Traditionally, health records kept by both private and public sectors have been vigorously protected by legislation and professional codes of conduct. But there are moves to give Australians the benefit of global and instant access to their health records. It is expected that, within a decade, four out of five Australians will have their personal medical details on a national electronic health record and be able to access them on their home computer using a unique identifier code—which I am sure is of no surprise to the member for Jagajaga, the shadow minister for health. The great benefit of this arrangement is that it will allow patients who are travelling interstate or internationally to check their medical record and details if they find themselves suddenly needing treatment. It will also enable doctors, hospitals and pharmacists to access the health records of patients they are treating who have opted into the system. In some instances it could save lives.

The drawback of this system is the threat it poses to individual privacy. There is a concern in Australia—perhaps justifiably so—of just how secure the Internet is. A recent international survey by credit card company American Express shows that most consumers prefer to purchase goods in retail shops rather than over the Internet because of fears about online security and privacy. In the Australian component of the survey, just over 85 per cent of the 1,200 Australian respondents said they were concerned about security and privacy when they made online financial transactions or purchases. Nearly 80 per cent of Australian respondents said they used the Internet as a research tool to investigate products on the market before visiting the retail outlet and purchasing the product there. These trends in the Australian market were reflected in the survey's global results that included 11,000 people in 10 countries.

The provisions of this bill should help address some of these concerns and provide a boost to Australian e-retailers and perhaps give them a competitive advantage over their international counterparts. Personal information collated by businesses on their clientele is generally used for marketing purposes to generate further sales. But personal information can also be abused due to corporate espionage. According to a report by PricewaterhouseCoopers in 1999, Fortune 1000 companies recorded $US45 billion in losses as a result of corporate espionage. Experts in the field believe that computer penetration is one of the most common external methods of stealing corporate information. This means that corporate clients are exposed to having their confidential information stolen and then used for unintended purposes. These are all legitimate consumer concerns. If Australia is to be a beneficiary of thriving e-commerce, it is essential that we ensure the e-commerce consumers' privacy has a reasonable level of protection from a framework of workable laws. This bill goes a long way to achieving this by helping to establish a new approach to the protection and handling of personal information in the private sector.

There has been a lot of comment generated in the media and by the opposition about the mechanics of this bill. We just heard from the shadow minister, the member for Barton, on this subject. Some interested parties advocate the insertion of retrospective provisions in this legislation. This suggestion lacks any degree of pragmatism. A retrospective clause would involve enormous compliance difficulties for the private sector. In some cases it would be a quite prohibitive condition. It is also worth noting that a retrospective requirement of this nature was not considered necessary when privacy legislation for the public sector was debated in parliament. It is difficult to see how you could argue that a retrospective requirement was suitable for the private sector but not for the public sector.

Another concern which has been raised is that the penalties prescribed for breach of this legislation are not sufficiently prescriptive. This is not the case. The Privacy Commissioner has the capacity to make a determination in favour of the person who makes a complaint and can order that compensation be paid, or that the offending conduct not be repeated, or that a specified amount for loss and damage be paid to the complainant individual. I understand that to date the Privacy Commissioner has been able to reach resolutions between parties based on negotiation and agreement without having to resort to heavy-handed threats.

Some people have criticised this bill for making pragmatic exemptions for some small businesses. This fails to acknowledge the fact that the Attorney-General has the authority to make the provisions of this bill apply to

cover small business via regulation in instances based on the recommendations of the Privacy Commissioner. It also fails to recognise that the exemption does not apply to small businesses that provide a health service and hold health information or businesses that trade personal information. The bill before the House addresses all these concerns. This bill provides a comprehensive privacy regime that will cover the private sector for the first time. This regime will protect consumers by ensuring that personal information is collected, stored and handled fairly by organisations in the private sector. It will also aid Australian small business in e-commerce by giving them a competitive advantage over their international competition that does not have sufficient privacy protection measures in place for consumers.

I would like to speak more about the bill. However, as I understand it, the opposition has made available a proposed draft of amendments only this morning, which is a considerable time after the debate, which makes it difficult to analyse them at this very late stage. I am concerned at the apparent inappropriateness of this conduct and whether the amendments are proposed as a serious contribution to policy development or as some form of mischief-making by the shadow Attorney-General, who only referred to them in this House less than 30 minutes ago. If the opposition were serious about privacy protection, surely they would have given the government more time to consider the amendments they are proposing.

The bill was introduced in April and the government circulated its proposed amendments on 4 September. The opposition have had ample time to consider them and to reach a position, yet the government has not been given the courtesy of seeing the opposition's proposed amendments until after the debate has already started. I understand that the Labor Party are very exercised at the moment with matters to do with the Queensland Labor Party and electoral enrolment integrity, and I accept that they may not have been able to get their minds around the necessary amendments to the bill that they are proposing. But, still, the government does feel that they could have extended us the courtesy of an earlier acknowledgment of their amendments. Even if the government were of a mind to consider some of the proposed amendments, it could not reasonably be expected to do so in the ridiculously short time provided by the opposition. The opposition should affirm their support for maintaining individual privacy by supporting the bill. This bill is a major step forward in the challenge of protecting individual privacy in an increasingly technological environment. This bill will help meet this challenge. I commend the bill to the House.