

Corporate & Commercial Brief May 2009



IN THIS ISSUE:

Update: Regulation of Electronic Contracts	1	Barefoot in Australia: Are you using your trade mark?	4
Direct Marketing: Guidance on the Interaction of the Spam and Privacy Acts	2	Current Status of Australia's Privacy Laws	5
Under Employment: When are Patents Protected?	3		

UPDATE: Regulation of Electronic Contracts

The Australian Government, in consultation with the States and Territories, is currently considering whether Australia should accede to the United Nations Convention on the Use of Electronic Communications in International Contracts 2005.

Implementation of the Convention in Australia would require amendments to extend and update Australia's current uniform electronic transactions regime. Such changes would be likely to affect organisations that use electronic means of communication in the formation or performance of business contracts.

The *UN Convention on the Use of Electronic Communications in International Contracts 2005* was adopted by the UN General Assembly on 23 November 2005. The purpose of the Convention is to facilitate international trade by offering practical solutions for issues that arise from the use of electronic communications in the formation or performance of contracts between parties located in different countries.

The Australian Government is now considering whether to implement the terms of the Convention into Australian law. The Attorney General's Department has received, and is considering, comments on its consultation paper entitled '*Australia's Accession to the UN Convention on the Use of Electronic Communications in International Contracts 2005 – Proposed Amendments to Australia's Electronic Transaction Laws*'.

Amendments are proposed to both State and Federal laws that regulate electronic transactions. It is contended that the proposed amendments will modernise the current laws, increase the certainty of international electronic trade and promote the growth of cross border online commerce.

Some practical implications of the proposed amendments are:

Electronic Signatures - Electronic signatures may be used in electronic communications either to represent a party's intention to be bound by the terms of the communication or as a tool to verify the party's identity within the communication. It is recommended that only electronic signatures that indicate a party's intention to be bound by the terms of an electronic contract may be enforceable. For example, the use of an 'I Agree' field within an electronic contract may provide sufficient indication of a party's intention to be bound by the terms of the contract.

Automated Message Systems - Many electronic transactions lack a human element as they are facilitated by the use of an automated message system ("AMS"). In other words, a contract may be formed by a party interacting with an AMS that acts on behalf of the other party. For example, if a party orders goods through a website, the transaction may be facilitated by an AMS whereby the vendor receives and confirms the order via

its e-commerce software. It is recommended that the current laws be amended to clarify that transactions that are formed by the use of an AMS are valid.

It is further recommended that a party employing the use of an AMS on an electronic platform be required to provide an opportunity for its customers to correct potential input errors. This may be achieved through the use of a 'confirmation screen' which provides the individual with an opportunity to correct information before executing the electronic contract.

What should you do?

It would be prudent for organisations to consider whether their contracting procedures are in accordance with the proposed recommendations. We will be monitoring the progress of the proposed amendments, further details of which are also available at "http://www.ag.gov.au/www/agd/agd.nsf/Page/Copyright_Australiane-commercereview-UNconventiononelectroniccommunications".

For further information please contact **Tania Zordan**, Partner on +61 2 9225 2551 or zordant@kempstrang.com.au.

Direct Marketing: Guidance on the Interaction of the Spam and Privacy Acts

Recent guidance by the Privacy Commissioner details how organisations may engage in direct marketing initiatives with their past, present and potential customers. Organisations should review their marketing activities in light of the Privacy Commissioner's recommendations.

The Privacy Commissioner recently released Privacy Sector Information Sheet 26 – *Interaction between the Privacy Act and the Spam Act*. The Information Sheet provides guidance on how the *Spam Act 2003* (Cth) and the *Privacy Act 1988* (Cth) interact to regulate the dissemination of electronic commercial messages from organisations.

The Acts overlap and interact with each other, in particular, in the area of electronic direct marketing. The Information Sheet is aimed at organisations that conduct electronic direct marketing via email, SMS, instant messaging or other wireless technologies.

The Information Sheet provides clarity in respect of inconsistencies such as those outlined below:

Consent

Under the Spam Act, an organisation must obtain an individual's consent before disseminating its commercial electronic messages. This consent may either be *express* or *inferred*.

By contrast, the Privacy Act provides that an individual's personal information must only be used for direct marketing purposes with the consent of the individual. This consent must be either express or implied.

The overlap in respect of consent manifests an inconsistency as to whether, in the absence of express consent, an organisation is to obtain inferred consent (as required under the Spam Act) or implied consent (as required under the Privacy Act) to disseminate commercial electronic messages.

National Privacy Principle 2 of the Privacy Act ("NPP 2") clarifies this inconsistency as it permits the use or

disclosure of an individual's personal information if it is authorised under the law. Accordingly, the rule of 'inferred' consent, as authorised by the Spam Act, overrides the requirement of 'implied' consent under the Privacy Act in respect of commercial electronic messages.

Inferred consent may occur through the organisation's existing relationship with the individual, where there is a reasonable expectation of receiving direct marketing messages, or where an individual's email address is freely available.

Organisations should obtain the individual's consent to, firstly, the collection of its personal information and, secondly, to *disseminate* the electronic commercial messages to the individual.

Impracticality

Further, NPP 2.1(c) of the Privacy Act provides that an individual's personal information may be used or disclosed for direct marketing purposes if the consent of the individual is impractical to obtain. As no such concession is provided under the Spam Act, it is recommended that commercial electronic messages not be sent if an individual's consent cannot be obtained.

Additional obligations under the Privacy Act

The Privacy Act imposes further obligations that must be satisfied in respect of commercial electronic messages that are not required by the Spam Act.

When personal information is collected by an organisation for the purpose of direct marketing, NPP 1.3 of the Privacy Act states that the organisation must take reasonable steps to provide the individual with details of the organisation and its handling procedures in respect of

the information collected. Further, should an organisation collect personal information of an individual from a third party, the organisation must take reasonable steps to ensure that NPP 1.3 has been complied with.

Additionally, the Privacy Act requires collecting organisations to take reasonable steps to ensure that the personal information they hold remains secure, and to provide opportunity for individuals to access and correct such information upon request.

Exemptions under the Spam Act

Certain commercial electronic messages may be exempt or partially exempt from the Spam Act, however, the use of personal information to send such messages may still be governed by the Privacy Act. Accordingly, the Information Sheet provides that electronic messages

that are exempt under the Spam Act should continue to identify the sender and provide its contact details to comply with the Privacy Act.

What should you do?

The Information Sheet provides guidance on how an organisation can comply with the requirements of both the Privacy Act and the Spam Act when engaging in electronic direct marketing initiatives. Should your organisation's marketing activities be governed by both Acts, it would be prudent to ensure that they are in accordance with the recommendations contained in the Information Sheet.

For further information please contact **Tania Zordan**, Partner on +61 2 9225 2551 or zordant@kempstrang.com.au.

Under Employment: When are Patents Protected?

The importance of careful and thorough intellectual property planning by employers, and the critical significance of properly drafted employment contracts, was confirmed recently by the Federal Court. Public and private sector entities engaged in research activities are advised to review their employment contracts and consider how effectively they are protecting their valuable intellectual property.

In the 554-page decision of *University of Western Australia v Gray* (No 20) [2008] FCA 498, the Federal Court examined the question of who owns the intellectual property in inventions created by an inventor whilst under an employment contract.

Professor Gray was employed at the University of Western Australia ("UWA") to teach and conduct research. During the period of employment, between 1985 and 1999, Professor Gray developed various novel treatments for cancer. Whilst employed by the UWA, Professor Gray co-founded a public company, Sirtex Medical Ltd ("Sirtex"). In 1997, Professor Gray transferred intellectual property rights in his inventions to Sirtex.

The UWA claimed that any purported transfer of the patent rights was a breach of Professor Gray's contractual and fiduciary duties to the UWA. It was alleged that, within Professor Gray's employment contract, there was an implied term as to the

UWA's ownership of IP rights over any inventions developed by Professor Gray whilst under employment with the UWA.

Justice French accepted that inventions made by an employee in the course of employment, undertaking work which the employee is engaged to do, would be the property of the employer through an implied term in the employment contract. His Honour cited well-established Australian, UK and US case law in concluding that such a term may be implied in circumstances where the employee is doing what he or she has been engaged or

instructed by the employer to do, during work hours and using the materials or resources of the employer.

In the present case, French J held that, under the terms of his employment, Professor Gray was employed "to research". His Honour held that academic staff are not under an implied duty "to invent" (even if it is possible that research may lead to invention). Accordingly, there was no term implied into the employment contract as to the ownership of the IP rights in the inventions created by Professor Gray. However, French J noted that where an employee was specifically retained to produce an invention, such a term could be implied into the contract.

His Honour drew a distinction between academic employment, where work is usually carried out for public knowledge and dissemination, and employment with industrial or commercial entities, where work would ordinarily be carried out for the commercial exploitation of inventions by the employer. A court may more readily imply a term vesting the IP rights in the employer in the later instance. His Honour noted that:

"the question... really reduces to a consideration of the nature of the particular contract by reference to the business or activity of its employer and the scope of the employee's employment in relation to that business or activity."

The UWA has indicated that it intends to appeal the decision.

What should employers do to protect their IP assets?

The Federal Court decision has significant ramifications for public and private sector institutions, where employees are engaged in research as well as other work activities. Employers should recognise that terms as to IP ownership will not, as a matter of course, be implied into employment contracts, and should ensure that contracts

specifically provide that all IP rights (including patents, trade marks, registered designs and copyright) will vest in the employer. Consideration should be given to the specific nature of each employee's role, and whether intellectual property may be generated during the course of employment.

For further information please contact **Tania Zordan**, Partner on +61 2 9225 2551 or zordant@kempstrang.com.au.

Barefoot in Australia: Are you using your trade mark?

A landmark trade mark case was handed down by the Federal Court last year with significant ramifications for companies seeking to enter the Australian marketplace. Registered trade mark owners are advised to carefully consider what constitutes "use" of their mark, and how quickly they commence using it, to ensure that they retain valuable intellectual property protection.

In 2005, California-based E & J Gallo Winery ("Gallo"), the second largest wine-producing company in the world, acquired the Australian registered trade mark "BAREFOOT" in relation to "wines". In early 2006, Gallo entered into discussions with McWilliams Wines for the sale of Barefoot wines in Australia. In 2007, Gallo licensed its "BAREFOOT" mark to McWilliams Wines, and shortly thereafter two varieties of Barefoot wines were placed onto the Australian market. Prior to that time, a small number of Barefoot wines had been sold in Melbourne by an unrelated wine wholesaler. In January last year, Lion Nathan launched a new beer into Australia under the trade mark "BAREFOOT RADLER". Gallo claimed that Lion Nathan infringed its trade mark by using a deceptively similar mark for its own product.

Were the marks deceptively similar?

Justice Flick agreed that "BAREFOOT" and "BAREFOOT RADLER" were deceptively similar marks. However, His Honour went on to extensively consider the two products (wine and beer), specifically examining the processes involved in producing each beverage, how and where they are sold and marketed, and the manner of consumption of each. On those grounds, Flick J did not consider that wine and beer are of the same description, and therefore there was held to be no trade mark infringement by Lion Nathan.

Interestingly, Flick J also upheld the Trade Marks Act 1995 (Cth) section 120(2) defence to infringement raised by Lion Nathan, finding that although the "BAREFOOT RADLER" mark was deceptively similar to the "BAREFOOT" mark, the manner in which it was used was not likely to deceive or cause confusion. His Honour found that the circumstances and environment in which each product was sold was relevant in determining the likelihood of consumer confusion. Section 120(2) is rarely raised judicially, and the decision is likely to encourage the defence in relation to future trade mark infringement.

Non-use of the Gallo mark

In 2007, Lion Nathan sought to have Gallo's "BAREFOOT" mark removed from the trade marks register for non-use for a continuous 3-year period. This was heard as part of the Federal Court proceedings.

Gallo raised several factors to demonstrate the requisite "use" of the mark in Australia during the relevant period:

1. The sale of Barefoot wine by the Melbourne wholesaler; and
2. The negotiations that had taken place between Gallo and McWilliams Wines for distribution of Barefoot wines in Australia.

The Court held that the sale of Barefoot wines was not due to any "use" or involvement by Gallo. The wine had found its way onto the Australian market via Germany, and Gallo in no way controlled the export, import or sale of the wine beyond the point of sale in the United States. Gallo had not "projected" the wine into the Australian market during the non-use period. Only use by the trade mark owner or authorised users is relevant to determining "use" in Australia, and Gallo's purported use was held to be insufficient. The Court held that any steps taken by Gallo to launch Barefoot wines into the Australian market were preliminary and preparatory only. Mere intention to use the mark in Australia was not "use" sufficient to defeat an application for removal for non-use.

What you should do?

Not surprisingly, given the ramifications of the decision on Gallo's plans to enter the Australian market with its Barefoot wines, Gallo is appealing the decision. This case serves to highlight that it is vital to use your trade mark in order to retain the protections derived from registration. When looking to enter the Australian market, it is important to commence using a registered mark as soon as possible. Non-use will leave your registered mark vulnerable to removal from the register.

For further information please contact **Tania Zordan**, Partner on +61 2 9225 2551 or zordant@kempstrang.com.au.

Current Status of Australia's Privacy Laws

The purpose of this briefing is to provide a broad general overview of some of the proposed changes to Australia's privacy laws and when they are expected to be implemented.

By way of recap, the Commonwealth Privacy Act was enacted in 1988. Substantial amendments were made to that Act by the enactment of the Privacy Amendment (Private Sector) Act 2000 which imposed privacy obligations on private sector organisations. It was at this stage that the operation of the Privacy Act became more widespread.

On 31 January 2006, the Australian Law Reform Commission ("ALRC" or "Commission") received Terms of Reference from the Australian Attorney-General for an inquiry into the extent to which the Privacy Act and related laws continue to provide an effective framework for the protection of privacy in Australia.

In its review, the Commission focussed on the shortcomings of, and potential improvements which could be made to, the Privacy Act.

On 11 August 2008 Special Minister of State, John Faulkner released the ALRC's report For Your Information: Australian Privacy Law and Practice and announced the government's plan to bring Australia's privacy laws into the 21st century. The report is 2,700 pages and includes 295 recommendations. It is the largest ever paper and investigation by the ALRC, and still doesn't cover everything.

The implementation of a full set of new privacy laws is expected to take 4-5 years. Following the extensive investigations by the ALRC, Australia is expected to be leading the world in this area.

To set the scene, following is a recap of some of the main provisions of the Privacy Act:

Overview of the Privacy Act

The Privacy Act and supporting regulations and guidelines regulate the collection, use, storage, disclosure of and access to 'personal information'.

'Personal information' is defined very broadly as information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. This could simply be a person's name, address, telephone number or date of birth.

The main parts of the Privacy Act are:

- Part III Division 2 which governs the operation of the Information Privacy Principles ("IPPs"), regulating the collection, use, storage, disclosure of and access to 'personal information' by public sector organisations;

- Part III Division 3 which is similarly concerned with information privacy and governs the way the private sector must deal with personal information under 10 principles known as the National Privacy Principles ("NPPs") and/or approved privacy codes;
- Part III Division 4 which is concerned particularly with the collection and storage of tax file numbers; and
- Part IIIA which governs the use of information by those who provide credit to individuals.

The NPPs set the minimum standards among the private sector for the collection, use, disclosure, security and access to personal information relating to a living person.

An organisation is defined in the Privacy Act to include an individual, a body corporate, a partnership, any unincorporated association or a trust.

There are express exemptions under the Privacy Act as it applies to private sector organisations including an exemption for small business operators, employee records, registered political parties, media organisations, State and Territory public sector agencies, government contractors and transfers of information between related bodies corporate.

A business is a small business if its annual turnover is \$3 million or less unless it gives or receives a benefit, service or advantage for the disclosure of personal information.

The NPPs apply to all 'organisations' regardless of whether they are also a credit provider or a file number recipient. Organisations may therefore be subject to multiple provisions.

Proposed Changes

The broad topic areas of recommended change are as follows:

Phase 1:

- National harmonisation of privacy law
- The effect of emerging information technology
- Credit reporting
- Privacy and health services

Phase 2:

- The limits of exemption from regulation
- Remedies for breach
- Cross-border transfer requirements
- Notifying data breaches

- Telecommunications
- Youth

The Government has advised that implementation of the recommendations for reform will occur in 2 phases. The first 4 of the above changes will occur in phase 1. The others need further consideration and will occur in phase 2.

Senator Faulkner indicated that the government is expected to legislate the 1st phase changes in 12 – 18 months (from August 2008). At a privacy symposium late last year Senator Faulkner indicated that the government was working through the recommendations and meeting with relevant persons. Before the end of 2008, the Department of Prime Minister and Cabinet would be conducting consultations with interested parties on key proposals, including the health and credit reporting areas. In early 2009 it will address the Standing Committee of Attorneys General with the government's views on the proposed reforms. It will then have further discussions to ensure the government is fully informed and any gaps are addressed.

Following is a brief discussion of each of the proposed changes:

National harmonisation of privacy law

The greatest emphasis of the report has been on addressing the overlapping and inconsistent federal, state and territory laws that regulate the handling of personal information.

There is overlap both between the state and federal laws and between the NPPs (that apply to private sector organisations) and the IPPs (that apply to public sector organisations) eg, where a private or non-profit organisation undertakes services outsourced to them by a government department.

In an attempt to streamline and simplify these principles, the ALRC proposes that there be one set of principles that apply to both public and private sector agencies, referred to as the Unified Privacy Principles ("UPPs").

To compensate for the differences between the IPPs and the NPPs, the UPPs will incorporate variations to the current obligations. For example, rules about the handling of sensitive information will be consolidated and amended to apply to both public and private sector bodies. Public sector agencies would be bound by the rules about sending information offshore, and should allow individuals to deal with them on an anonymous basis where this would be lawful and practicable, as is already provided for under the NPPs. All organisations will need to have their privacy procedures and privacy policy statements reviewed to ensure they comply with the new laws.

The ALRC recommends that the Privacy Act should be amended to specifically apply to the federal public sector and the private sector to the exclusion of state and

territory laws. The Commonwealth, state and territory governments should also establish an intergovernmental harmonisation scheme under which all Australian governments would agree to consistently adopt the key elements of the amended Privacy Act, including the new recommended UPPs. This agreement would also create a mechanism by which future amendments to the harmonised regime would be suggested and effected.

The changes have drawn on the existing "principles based" regulation recognizing that principles can be flexible, high level and allow for a greater degree of "future-proofing" but has also recommended a rules-based approach in the form of regulations and industry codes in particularly challenging areas, such as health and credit reporting.

In addition to primary legislation and regulations for complex areas, it recommends that the Office of the Privacy Commission, the Australian Communications and Media Authority and others be responsible for education and guidance, especially about the effect of emerging technologies as they arise.

The effect of emerging information technology

This was one of the main concerns to be addressed by the inquiry. The way in which certain types of new technology falls within the current privacy laws has often been uncertain. For example, whether information gathering software (eg cookies) that collects information about a computer rather than an individual is "collecting personal information" and whether website hosts are "collecting" personal information that users post on online discussion forums.

As part of its investigations, the ALRC considered a wide range of emerging technologies in depth and the way in which they deal with personal information.

The ALRC recommends the implementation of technology-neutral privacy principles, supported by a technology aware regulatory framework. It acknowledges that recent advances in technology (eg the internet, biometrics, digital phones and cameras and radio frequency identification, such as toll tags) have made it easier, cheaper and faster to collect, store and aggregate large amounts of personal information. However, it also acknowledges that technologies are evolving so rapidly that any specifically targeted provisions would be outdated fairly quickly.

It recommends that education and guidance should be developed by the Privacy Commission and others about the effect of emerging technologies (such as RFID tags and social networking sites) on individuals' privacy.

Credit reporting

Part IIIA of the Privacy Act, together with the Credit Reporting Code of Conduct currently regulate the use of credit information by credit providers throughout Australia. The Act is largely concerned with consumer credit and related transactions.

If an organisation prepares or maintains records containing personal information, which is not publicly available, for the purpose of providing information on an individual's credit worthiness or credit history to other parties, the organisation may be considered to be a credit reporting agency.

The Act regulates the information which credit providers can give to credit reporting agencies to keep in credit information files relating to an individual.

The information which can be recorded in a credit information file includes:

- (i) Any personal information given to a credit reporting agency reasonably necessary to identify the individual (eg name, sex, date of birth, address, current or last known employer and driver's license number);
- (ii) details of credit provided to an individual where the individual is at least 60 days overdue in payment and action to recover that outstanding payment has commenced;
- (iii) the fact that a cheque for over \$100 drawn by an individual has been presented and dishonoured twice;
- (iv) a record of any report by a credit provider that in its opinion, the individual has committed a serious credit infringement.

The ALRC's suggested credit reporting reforms include the introduction of a form of "positive credit reporting" permitting the collection and disclosure of the dates and types of credit accounts opened and closed and their limits and, subject to appropriate additional regulation, an individual's repayment history. Strict limits would apply to the use and disclosure of this information, including a prohibition on using this information for marketing purposes.

Privacy and health services

For the regulation of personal health information, the Commission has acknowledged that there are complex arguments for and against specific health privacy legislation. The Commission's proposed compromise is that health information principles and exceptions to the proposed unified privacy principles should be set out in regulations to be called the Privacy (Health Information) Regulations.

For those agencies and organisations that handle health information, the ALRC recommends that the Privacy Commissioner publish a document setting out the UPPs as amended by the new set of Privacy (Health Information) Regulations. This document would provide a complete set of privacy principles covering health information, as well as other personal information (without unduly lengthening the UPPs themselves for the many organisations that do not handle health information).

Unique healthcare identifiers or a national Shared Electronic Health Records scheme should be established

under specific enabling legislation if the scheme goes forward.

The limits of exemption from regulation

One of the main criticisms of the Australian privacy laws is that there are more exemptions than there are laws.

To address this and bring Australia into line with other jurisdictions, the Commission recommends that the existing exemptions in the Privacy Act relating to employee records, political parties and small business be abolished and a more restricted exemptions apply to media organisations.

In relation to the employee records exemption, the ALRC recognises that there is a real potential for individuals to be harmed if employees' personal information is used or disclosed inappropriately and that employees may be under economic pressure to provide personal information to their employers.

Accordingly, organisations will need to review procedures for dealing with employee records and the type of information kept in them.

Remedies for breach

Another common criticism of the current Privacy Act is that it has no "teeth" and that "a right with no remedy is no right at all".

It is recommended that a wholly new privacy right be introduced by statute that allows individuals to obtain remedies where their privacy is invaded in a highly offensive way. The right would require both a reasonable expectation of privacy and a highly offensive interference with that expectation. Where the public interest in maintaining the right to privacy was outweighed by other public interests (such as freedom of expression, or the interest in informing the public about matters of public concern) no remedy would be available.

In other jurisdictions, this remedy is typically used by celebrities enforcing their right to privacy from the paparazzi. By contrast, most of the submissions received by the Commission related to concerns regarding the privacy of an average person for example, a photograph taken on a mobile phone in a dressing room being published on the internet. Accordingly, the new legislation is likely to attempt to address a slightly different type of claim to that of other jurisdictions.

The relationship between the right to privacy and existing rights (eg breach of confidence and defamation) is yet to be resolved.

It is also recommended that further remedies be made available to the newly named Australian Privacy Commission including enhanced powers to direct those in breach to take specified actions, to enforce those directions and to seek civil penalties where serious or repeated breaches occur.

Cross-border transfer requirements

It is recommended that the privacy laws be amended to provide that organisations and agencies that transfer personal information outside Australia remain responsible for the protection of that information unless:

- the agency or organisation believes that the recipient is subject to privacy protections that are of a similar standard to Australia's;
- the individual consents to the transfer; or
- the agency or organisation is required or authorised by law to transfer the personal information.

Individuals seeking to enforce their privacy rights would be assisted by Australian entities remaining responsible for their actions. However, the first exemption outlined above lacks certainty and has the potential to significantly limit the circumstances in which an organisation would be held accountable. This proposal requires further consideration.

If implemented, this change would have a significant impact on organisations that outsource operations (eg call centres) overseas. Such organisations will need to carefully consider their procedures for sending personal information overseas.

Notifying data breaches

The ALRC recommends that organisations and agencies be obliged to notify affected individuals and the Privacy Commissioner if they believe that an unauthorised acquisition of information held by them will result in a real risk of serious harm to any individual.

Telecommunications

The ALRC recommends that Part 13 of the Telecommunications Act 1997 (Cth) (relating to the privacy of telecommunications information) should be simplified.

The regulation of telecommunications interception and access and telecommunications regulation generally should be reviewed to ensure it is effective in light of technological change and public perceptions. The Australian Communications and Media Authority (ACMA) should also provide guidance on the privacy issues raised by new technologies such as location-based services, Voice over Internet Protocol (VoIP) and electronic number mapping.

Youth

The report provides guidance on the circumstances in which young people may be presumed to be capable of giving consent, making a request or exercising a right of access concerning their personal information.

The issue is not yet resolved. The outcome will be important for schools and all organisations that may collect personal information relating to young people, including in online discussion forums.

Schools should clarify how information about students will be handled, including when it will be disclosed to, or withheld from parents.

It is apparent from the above broad overview that the proposed changes are significant and will affect most Australian organisations in some way.

For further information please contact **Tania Zordan**, Partner on +61 2 9225 2551 or zordant@kempstrang.com.au.

Key Contacts:

For further information on our Corporate & Commercial Brief, or our firm in general, please contact:



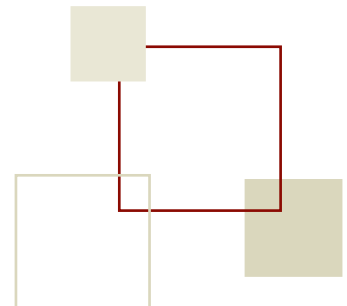
Tania Zordan, Partner

Tel: (02) 9225 2551
Fax: (02) 9225 2599
E: zordant@kempstrang.com.au



Daren Armstrong, Partner

Tel: (02) 9225 2585
Fax: (02) 9225 2599
E: armstrongd@kempstrang.com.au



Kemp Strang's corporate & commercial brief is intended to keep readers abreast of current legal and firm developments. It is not to be used or relied upon as a substitute for professional advice. Before acting on any matter, readers should consult with their advisors.

If you do not wish to receive further mailouts please email us at info@kempstrang.com.au or telephone Marianne Slocombe on 9225 2711.