LexisNexis™ Butterworths

Volume 10 Numbers 4 & 5

Print Post Approved 24437100049

Internet Law Bulletin

Contents

Information contained in this newsletter is current as at August 2007

LexisNexis™ Butterworths

Open source software takes a big step forward

Julian Lincoln FREEHILLS

The General Public Licence (GPL) is one of the most widely utilised software licences in the world. It is also one of the most important legal frameworks underpinning the open source software movement.

After several discussion drafts and a review process taking close to a year and a half, the Free Software Foundation finally released the new version of the GPL, version 3.0, on 29 June 2007. GPL version 3.0 is the first overhaul of the GPL since 1991.

Obviously, much has changed in the world since 1991 and so GPL 3.0 contains many changes and additions when compared to GPL 2.0. That said, the core 'copyleft' principles that everyone should be free to copy, change and distribute the source code of a GPL licensed program remains the same in GPL 3.0. GPL 3.0 seeks to clarify various potential ambiguities in GPL 2.0, and also introduces important new provisions around software patents, digital rights management and the 'tivoisation problem' of using hardware to lock down open source code.

As a general comment, GPL 3.0 is not an easy read. This is perhaps partly due to its US emphasis and drafting style, and partly due to the multitude of issues which the GPL seeks to address in a way most likely to be applicable and enforceable around the world.

This article begins with a short refresher on the GPL and the Free Software Foundation and what they stand for. The article then aims to provide an overview of the key changes and points to note in GPL 3.0, as compared to GPL 2.0.

Background

What is the GPL?

The GNU General Public Licence is published by the Free Software Foundation. The Free Software Foundation describes itself as 'dedicated to promoting computer users' rights to use, study, copy, modify, and redistribute computer programs. The FSF promotes the development and use of free software, particularly the GNU operating system … '.[1]

Put simply, the GPL is a software licence agreement designed specifically for open source code. A developer of a new software program can elect to license his or her code under the GPL, thereby contributing it to the open source community. A person who obtains through any means a software program licensed under the GPL is bound by the GPL, hence ensuring that any software created and distributed 'downstream' from the original work remains in the open source domain.

What is the GNU project?

The GNU operating system is a complete free software system, compatible with Unix. GNU stands for 'GNU's Not Unix'. The project to develop the GNU system was launched in 1983 and aimed to foster collaboration among software developers by removing proprietary restraints which prevent the free flow of source code.

What is 'free software' anyway?

Free software does not refer to free in the sense of no cost. Rather, free software refers to each user having the freedom to run, copy, modify and distribute the source code of the software. The Free Software Foundation defines free software as software which provides the following rights to all users:[2]

- the freedom to run the program, for any purpose (freedom 0);
- the freedom to study how the program works, and adapt it to your needs — access to the source code is a precondition for this (freedom 1);
- the freedom to redistribute copies so that you can help your neighbour (freedom 2); and
- the freedom to improve the program, and release your improvements to the public, so that the whole community benefits — access to the source code is a precondition for this (freedom 3).

There are many different open source licences. Note that not all licences which proclaim themselves as being a 'free software' or 'open source' comply with the FSF's definition of free software. Some of the better-known open source licences include the Apache licence, BSD licence, Netscape public licence and Intel open source licence.

Obtaining a copy of GPL 3.0

GPL version 3.0 is available from a number of sites, including:

- <www.fsf.org/licensing>; and
- <www.gnu.org/licenses/gpl.html>.

Core GPL principles remain the same

The 'copyleft' principles for which the GPL is famous have, not surprisingly, been retained in GPL 3.0. In summary, the philosophy underlying the GPL is that every person should be free to copy, change and distribute the source code of any software program which is distributed pursuant to the GPL.

One of the important consequences of this principle is that all source code of any software incorporating GPL licensed code which is distributed to third parties must also be made available. Clause 5 of GPL 3.0 sets out the conditions which apply to any distribution of code. In summary:

- the work must carry notice of the modification;
- it must be made clear that the work is distributed under the GPL;
- the entire work as a whole must be licensed to anyone who obtains it; and
- if the work has an interactive user interface, then certain legal notices must be displayed.

Important new concepts in GPL 3.0

Patent rights

One of the grey areas of GPL 2.0 was the impact of business process or software patents on software licensed under the GPL. This is because GPL 2.0 did not specifically address patent rights and therefore the scope of the licence beyond copyrights was not clear and open to debate. Since 1991, the patent landscape has changed significantly in a number of ways. Relevantly for the GPL, in many jurisdictions it is now possible to obtain patent rights over business processes (which, for example, may be implemented through software) and software itself. The ability for such patent rights to 'trump' the contractual copyright licence terms of the GPL had the potential to significantly weaken the underlying principles and enforceability of open source software licensing.

Indeed, the preamble to GPL 3.0 states that:

> Finally, every program is threatened constantly by software patents … [W]e wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

Clause 11 of GPL version 3.0 directly addresses this patent issue. Any person who contributes their copyrighted works to the community under the GPL grants a 'non exclusive, worldwide, royalty free patent licence' to any patent rights owned or controlled by that person to 'make, use, sell, offer for sale, import and otherwise run, modify and propagate' the software.

Clause 11 also addresses the situation when a person provides a software program knowingly reliant on a patent licence:

> If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients.

Where a patent licence has been granted to one recipient of a work, then clause 11 may act to automatically grant a patent licence to all persons who received the work as part of the same transaction or arrangement:

> If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

The practical effect sought by this drafting is to avoid discriminatory conduct by the patent licensor in relation to patent claims which apply to a software work covered by GPL 3.0.

Finally, the GPL now contains a provision which seeks to prevent a person distributing code under the GPL 3.0, who pays a third party for a 'discriminatory'[3] licence that would benefit its own customers using such code but not others. This restraint only applies to licences granted after 28 March 2007. This clause was reportedly inserted to address licensing or 'no suit' agreements between parties, such as the well-publicised arrangement between Microsoft and Novel, wherein Microsoft agreed to not sue customers of Novel's SUSE variant of Linux.

Digital rights management

The FSF has responded to the trend in many countries (including Australia) to enact legal regimes prohibiting devices designed to circumvent technological protection measures. Such regimes, coupled with digital rights management (DRM) technologies, posed a risk that open source projects could be 'locked up' behind DRM systems.

To address DRM technologies, clause 3 provides that:

> No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work.

Thus, one of the objects of the FSF is to ensure that any software which is licensed under the GPL cannot form part of a technological protection measure (TPM).

Tivoisation

'Tivoisation' (or 'tivoization' in the US) is a term which has been coined by the FSF and describes 'devices that are built with free software, but that use technical measures to prevent the user from making modifications to the software — a fundamental freedom for free software users'.[4] While many devices, especially consumer electronics devices, fit this description, it is the extremely popular (in North America) 'TiVo' device which has greatly agitated the open source community. TiVo uses open source software. While TiVo's manufacturer complies with GPL requirements by releasing source code changes back to the community, the TiVo device itself, through clever hardware, prevents users from modifying the software which runs on the device.

GPL 3.0 includes new provisions to prevent this practice, except where the device is one which cannot be updated — for example, where software is programmed into 'read only memory' at the time of manufacture.

This restraint is included in clause 6:

> If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient … the

> Corresponding Source conveyed under this section must be accompanied by the Installation Information.[5]

Significant drafting changes in GPL 3.0

Termination of licence

GPL 3.0 contains specific provisions confirming licence termination when the terms of the GPL are not complied with. These provisions are in part designed to remove any doubt as to termination of a GPL licence, and whether a recipient of a GPL licence receives only contractual rights or also receives a 'bare licence' to the copyright subsisting in the licensed works.

Clauses 8 and 9 now make clear that the only rights to a work covered by GPL 3.0 are the contractual rights set out in the licence itself.

Clause 8 also permits, in some circumstances, a person who breaches the GPL to cure the breach and continue using the affected code:

> However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.
>
> Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Importantly, 'Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License'.

Liability regime

As with version 2.0, GPL 3.0 contains broad liability disclaimer and limitation clauses.[6] The general gist of these provisions is that any software provided under a GPL licence is provided on an 'as is' basis, with no representations or warranties made, or liability assumed, by any author(s) of any code.

Notwithstanding the launch of GPL version 3.0, the previous version 2.0 will remain an important open source licence for many years to come. This is because software which was released under GPL 2.0 may remain licensed under GPL 2.0.

Attempts have been made in version 3.0 to broaden the drafting of the provisions to make them less 'US centric' and to accommodate local laws in other countries which may not permit such a total exclusion of liability.

GPL 2.0 remains important

Notwithstanding the launch of GPL version 3.0, the previous version 2.0 will remain an important open source licence for many years to come. This is because software which was released under GPL 2.0 may remain licensed under GPL 2.0.[7] Thus, the sheer volume of existing code in use which was licensed under version 2.0 ensures an important role for version 2.0 for the foreseeable future.

If given the option to use either GPL version 2.0 or 3.0, then careful consideration should be given regarding how the attributes of each licence type apply to your particular circumstances. For example, if you hold software patents, then the patent provisions in version 3.0 may make that version less appealing.

Related licence agreements

In conjunction with the new version of the GPL, the FSF also released a new version of the 'Lesser GPL' licence. The LGPL incorporates the GPL terms. The LGPL is designed for use with code libraries and importantly works covered by the LGPL can be used in commercial products. The Lesser GPL, and other FSF projects such as the Affero licence project, will be the subject of a subsequent article in this bulletin.

Careful consideration is important

It is important to carefully review the applicable licence terms before using, modifying and especially distributing any software which includes any open source code. Issues to be considered include technical and security issues, integrity of code, confidentiality of business information and processes, and, of course, the legal risks and consequences flowing from the use of open source software. ●

Julian Lincoln, Senior Associate, Corporate IP & Technology Group, Freehills, Melbourne.

Endnotes

1. See <www.fsf.org>.
2. See <www.gnu.org/philosophy/free-sw.html for further information>.
3. A patent licence is 'discriminatory' if 'it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License'.
4. See <www.fsf.org/iphone-gplv3>.
5 See clause 6 of the licence for the full provision, including definitions of 'User Product' and 'Installation Information'.
6. See clauses 15, 16 and 17.
7. Software originally licensed under GPL 2.0 will remain licensed under version 2.0, unless the author elects to 'upgrade' their licence to GPL 3.0.

The future impact of the internet on electronic discovery

Allison Stanfield E.LAW AUSTRALIA PTY LTD

Electronically sourced information has created an entirely new realm of discovery for litigators. Use of the internet has meant that vast quantities of electronic information can be exchanged instantaneously, with the content of such information often being prepared casually and without thought as to the long-term consequences of litigation.

During the 1980s, the use of litigation support systems meant that vast reams of paper could be imaged and that manually entered data could be used to assist with the indexing, cataloguing and analysing of discoverable materials. Over the last 20–25 years, such litigation support systems have become the norm for handling large discoveries. The internet has assisted the preparation of litigation by allowing research materials to be delivered online and litigation support systems to be accessed remotely by members of the legal team, including counsel, expert witnesses and even clients. Electronic discovery has expanded from the practice of rendering hard copy documents into a digital format, to the retrieval of electronic files in their native format, sorting through them to find what's relevant and discovering them without the need to reduce them to hard copy. Following on from the C7 litigation,[1] the Federal Court and the Supreme Court of NSW have introduced changes to court practices by decreeing that pre-trial discovery will take place electronically.

Chief Justice Spiegelman has stated that the 'only court-book documents that will be in hard copy will be those that are actually used and referred to in each case'.[2]

However, use of the internet in the business world has meant that the scope of discovery has increased significantly. Justice Sackville made this point in the C7 litigation,[3] where his Honour noted that 'mega-litigation … generates vast quantities of documentation in paper or electronic form',[4] and this scope may well increase in the future. On the other hand, however, technological developments on the internet will ensure that complicated systems being built today to deal with electronic discovery may be easier to use. Think about email in the early 1990s: one had to connect using an external modem; ensure that the AT&T string was correct; use a black-and-white interface to connect; and memorise and use a number of UNIX strings. Today, all one has to do is open one's email page and merrily send and receive email all day long. This simplicity of use will continue to be realised on the internet.

Developments on the internet will be in two areas: connectivity and content. Improvements in connectivity will mean that more devices can be connected to the internet, and improved features to access content will mean that identifying what is relevant for discovery will be simplified. In conjunction with this, court practice notes will provide that discovery must take place in electronic format, and that there is a non-waiver of privilege on documents subject to discovery.[5] This follows the American example of producing electronic documents in 'native' format after reviewing documents using search tools. The volume of information involved means that it is simply too cost prohibitive to review every document prior to discovery.

The future of the internet: connectivity

Today, electronically sourced information comprises the usual suspects, such as electronic files from file servers, laptops and desktop computers, and the ubiquitous email. However, it also includes a rapidly expanding realm of devices. In the corporate world, forensic and electronic discovery experts will look at the following during the information-gathering phase of a discovery: file servers, email servers, proxy servers, firewall logs, system logs, laptops/PCs, removable media (for example, USB memory sticks), backup media, fax servers, voicemail systems, PDAs/BlackBerries, mobile phones, iPods/MP3 players and digital cameras.

Information from home devices may also be relevant, particularly if staff members frequently work from home, or if there is a suspicion that information has been sent to a home device. Such devices may include laptops/PCs, removable media (for example, USB memory sticks), backup media, ISP records, iPods/MP3 players, digital cameras and mobile phones.

In the future, the list of devices may reduce in some areas and expand in others.

Some technical facts and figures

Currently, most computers that are connected to the internet do so by what is known as IPv4, comprising IP addresses that are 32-bit. This means that it is possible to express 4,294,967,296 different values. Over half a billion of those are unusable as addresses for various reasons, leaving a total of 3.7 billion possible addresses for hosts on the internet. As of 1 January 2007, 2.4 billion of those were in (some kind of) use; 1.3 billion were still available; and about 170 million new addresses were being given out each year. So, at this rate, by 2014 there will be no new IP addresses — sooner if the number of addresses used per year goes up.[6]

The next generation of the internet, known as IPv6, uses 128-bit addresses, which means that the total number of possible addresses allowed is 340,282,366,920,938,463,463,374,607, 431,768,211,456.[7]

So, what is the benefit of this 'new internet'? Geoff Huston sums up IPv6 as follows:

> IPv6 can allow for the resumption of a

network model that uses unique global addresses for each connected endpoint, for endpoint populations that can scale into the hundreds of billions. IPv6 is capable of embracing a device-dense world. The per-address cost can be reduced dramatically through the elimination of various forms of dynamic address translation technologies, as well as the elimination of the scarcity premium factor in IPv4 address mechanisms. Application complexity can also be reduced, and the diversity of application models can be broadened. This model of universal addressing allows for many forms of peer-to-peer networking models as well as supporting communication transaction security models that reply on end-to-end coherence. All these factors point to a networking model that supports simple and ubiquitous communications services which in turn supports utility device deployments. So the desired outcomes appear to point to simpler networks, simpler applications, larger populations of connected devices, more efficient services, and a broader diversity of service models. So the set of potentials presented by ubiquitous adoption of IPv6 presents a very compelling picture of benefits for a diversity of players in the industry.[8]

IPv4 has been driven by the computer market, which comprises the current internet and many other intranets which are not necessarily connected to the internet. This computer market has grown at an expediential rate, doubling approximately every 12 months. Most computers are attached to Local Area Networks (LANs) and most are not mobile,[9] although this is changing.

In 1995, Robert Hinden predicted that the next phase of growth of the internet would not be driven by the computer market, but rather by 'nomadic personal computing devices' that will require networking capability, will support a variety of types of network attachments and, when disconnected, will use wireless networks. These devices will need a common protocol which can work over a variety of physical networks. 'These types of devices will become consumer devices and will replace the current generation of cellular phones, pagers, and personal digital assistants', predicted Hinden.[10] Indeed, we are already seeing these 'one-stop shop' devices with the new iPhone from Apple, which comprises a phone, MP3 player, camera and mini-PC, and also connects to the internet, browses the web, and downloads and plays audio and video files. Such devices will require an internet protocol which imposes a low overhead and supports auto configuration and mobility as a basic element.

The impact on e-discovery

The effects on electronic discovery are that PDAs/BlackBerries, mobile phones, iPods/MP3 players and digital cameras are replaced by just one device.

Another market is networked entertainment, especially in the realm of internet TV, where it is possible for each TV to become an internet host — with the result that the differences between a computer and a television will diminish. The effects on electronic discovery are that the TV may indeed become a device that needs to be reviewed as part of discovery, depending on the type of litigation involved.

Another market which could use the next-generation IP is device control. This consists of the control of everyday devices such as lighting equipment, heating and cooling equipment, motors and other types of equipment which are currently controlled via analog switches and in aggregate consume considerable amounts of electrical power. The effects on electronic discovery may be that log files for the control of such equipment may indeed be relevant, especially where the quantum of a user's office or household expenditure is relevant — for example, if there is a dispute as to the volume of electricity used.

The future of the internet: content

The way in which discovery is carried out has changed dramatically over the last 20 years and, certainly, more rapidly over the last five years. The advent of computer technology, combined with the ease with which information can be exchanged via the internet, has meant that new ways to handle and process electronic documents have had to be developed. To this end, a number of service providers and vendors have developed tools to enable electronically sourced data to be 'processed' for upload into traditional litigation support systems. However, these litigation support systems were designed with a view to dealing with hard copy materials that had been converted into an image format with metadata about each document stored in databases.

In the future, lawyers will be more experienced in dealing with electronic data for discovery. The problem lawyers currently face is that discoverable materials, particularly electronic materials, are frequently provided in an extremely unstructured way. Often, the only way to deal with vast amounts of material is to:

- cull irrelevant material — this can be undertaken by ignoring certain file 'types', that is, those computer files that are designed to run software and otherwise do not contain relevant content;
- de-duplicate — this is quite a simple process with electronic material, since an electronic 'fingerprint' can be generated for each electronic file and compared with other electronic files;
- identify a particular custodian's files — only email repositories of certain persons may be relevant;
- identify timelines — files generated between particular dates only may be relevant (however, this process must be undertaken carefully, given that dates can be updated automatically by computer processes); and
- undertake keyword searches — it is predicted that the methods of searching across vast repositories will become more sophisticated, especially where web content is concerned.

What about 'deleted' files?

Deleting files does not necessarily mean that files have been deleted from a computer's hard drive; rather, deleting files simply makes space available on a computer hard drive for those files to be overwritten, since every computer's storage device contains files (used space) and free space (unused space).

The only ways to effectively destroy electronic files are the following:

- overwriting;

- physical destruction, including via heat; and
- magnetic destruction.

Overwriting can be undertaken over a period of time, since each time a computer is used it may modify metadata of files in used space and may overwrite previously deleted data in unused space. However, in order to be sure files are overwritten on a computer hard drive, an overwriting software program should be used which will overwrite data with a specific or randomly generated pattern of data. If run properly, it will make the data unrecoverable by computer forensics experts, although there may be ways to tell the date, time and specific program used to conduct the wiping.

Physical destruction includes dropping a hard drive, setting it on fire (although this is only successful if the drive is exposed to heat in excess of 300 degrees Fahrenheit), submerging it in water or shredding it.

Magnetisation involves using a degaussing device (as opposed to an ordinary magnet), which must be strong enough to disrupt the magnetic orientation of the data on the platters.

A responding party may take issue with documents that have been destroyed, particularly if it is alleged that the documents were destroyed in 'anticipation' of litigation — as was the case in *McCabe v British American Tobacco Australia Services Ltd* (*McCabe v BATAS*),[11] where the court imposed sanctions on the defendant for having destroyed documents. Although the decision of Eames J was overturned on appeal[12] and a re-trial ordered, the re-trial never took place and there remained unanswered questions as to the effect of destroying documents where litigation is 'anticipated'.

Since the *McCabe v BATAS* case, the legislature has closed the gap with respect to the possible destruction of documents where litigation is anticipated. The *Crimes (Document Destruction) Act 2006* (Vic) (the DDA) amends the *Crimes Act 1958* (Vic), and the *Evidence (Document Unavailability) Act 2006* (Vic) (the DUA) amends the *Evidence Act 1958* (Vic) and the *Victorian Civil and Administrative Tribunal Act 1998* (Vic).

The offence created in the DDA applies where a person knows that documents are reasonably likely to be required in any *ongoing* or *potential future* legal proceedings, and destroys or conceals the documents with the intention of preventing the documents from being used in a legal proceeding. Individuals and corporations can be prosecuted; for corporations, the conduct, knowledge and intention of officers of the corporation are automatically attributed to the company. The Act also introduced a 'corporate culture' test, but offers a limited defence of 'due diligence'.

The DUA deals with the document unavailability in a civil proceeding, and the document is unavailable if it is, or has been but no longer is, in the possession, custody or power of a party to a civil proceeding, and the document has been destroyed, disposed of, lost or concealed, or rendered illegible, undecipherable or incapable of identification, whether before or after the commencement of a proceeding.

The difference between the DDA and the DUA is that the latter Act is not concerned with how the document was destroyed. Similarly, if a copy of the document is available, then the DUA will not apply.

When certain evidence may not be adduced, the court has the discretion to make rulings or orders such as:

- drawing an adverse inference;
- ruling that a fact in issue between the parties be presumed to be true in the absence of evidence to the contrary;
- rejecting the admission of documents where their reliability has been tainted by another document's unavailability;
- striking out all or part of a defence or statement of claim; or
- reversing the burden of proof in relation to the issue being covered by that document.

Any one of these orders could change the entire outcome of a case. Before exercising its judicial discretion, the court must have regard to:

- the circumstances in which the document became unavailable;
- the impact of the unavailability of the document on the proceeding, including whether the unavailability of the document will adversely affect the ability of a party to prove its case or make a full defence; and
- any other matter that the court considers relevant.

The Act operates prospectively and retrospectively. In the retrospective sense, the Act may be applied if the documents which are relevant to proceedings commenced on or after 1 September 2006 became unavailable before that date.

Other legislative provisions that are relevant include:

- reg 177 of the *Legal Profession Regulation 2005* (NSW) — provides that a legal practitioner must not give advice to a client to the effect that a document should be destroyed if it is 'likely that legal proceedings will be commenced in relation to which the document may be required';
- s 39 of the *Crimes Act 1914* (Cth) — provides offences for where a person intentionally destroys a document knowing that it is required in evidence in a judicial proceeding;
- s 243 of the *Criminal Law Consolidation Act 1935* (SA) — provides offences for fabricating, altering or concealing evidence; and
- reg 177 of the *Legal Profession Regulation 2002* (NSW) — provides that a legal practitioner must not destroy or give advice to a client to destroy document(s) where it is likely that legal proceedings are to be commenced.

If documents are destroyed in accordance with a bona fide document retention policy at a time when litigation is not likely or anticipated, then a defendant will have a better chance of showing that documents were destroyed in good faith. However, if document destruction is conducted in a seemingly haphazard or random manner, then innocent deletions may seem sinister. If electronic documents are destroyed in accordance with a document retention policy, then one of the destruction methods mentioned above should be employed.

Searching across electronic sourced information

Keyword searching is the key to locating relevant material and many hours can be spent going backwards and forwards between legal representatives to ensure that material is not being excluded by search terms. However, keyword searching remains limited by its very nature. The next generation of search is contextually and linguistically smarter, thinking more like a human and able to chase the meaning of a search term through a document instead of just looking for a handful of words. These search engines put keywords into context in order to give them meaning when looking for a document.

Clustering is another tool used in electronic discovery. This is where documents pertaining to a particular theme may be clustered together and marked as relevant or irrelevant as the case may be. For example, a user may wish to search on all emails with the subject 'latest version contract'. Upon review, the user can determine that all emails with that title are relevant to the issue of, say, 'contract finalisation'. Clustering allows lawyers to review document repositories quickly.

The key to locating and finding information on this expanded version of the internet lies in what is known as the 'Semantic Web', which is Sir Tim Berners-Lee's vision of the future (Sir Tim is recognised as the creator of the world wide web). Presently, much of the content on the internet is unstructured data. One of the tools of the Semantic Web is what's called the Resource Description Framework (RDF), which will enable documents on the web to be given structure and, therefore, meaning. The result is that important information can be marked up, or tagged, and once this is contained within documents, software agents can pick up and use the tagged information, much like information contained within a database. For example, one way to represent the notion 'the sky has the colour blue' using RDF is as specially formatted strings: a subject denoting 'the sky', a predicate denoting 'has the colour' and an object denoting 'blue'.

Imagine the possibilities if each document were marked up with items such as 'document type' (for example, contract), 'document author' (for example, XYZ Pty Ltd) and 'document date' (for example, 1 Jul 2007). This is all possible using XML (eXtensible Markup Language). XML allows text within documents to be 'marked up'. For example, using HTML (HyperText Markup Language), the most common markup language used on the web at the moment, the following may be marked up within a document: <FONT Colour='Red">I agree to give you a peppercorn in exchange for your services.</FONT>

Using XML, the markup could be as follows: <CONTRACT Colour='Red">I agree to give you a peppercorn in exchange for your services.</CONTRACT>.

Both phrases will appear in red; however, XML is much more powerful in that it gives *meaning* to the words. RDF is a framework to give meaning to words in a standard way.

Combining connectivity and content: how will these work in the future?

Presently, electronic discovery comes in many different formats but, commonly, documents end up being one or more of the following file formats:

- email (Microsoft Outlook or Lotus Notes are the most common);
- word processing files (Microsoft Word);
- spreadsheets (Microsoft Excel);
- presentations (Microsoft Powerpoint Presentations); and
- PDF (Adobe Portable Format).

The common theme to the above is Microsoft. Therefore, if all documents created in our offices today can be created tomorrow using XML, then the knowledge domain is being created as we create documents. The key to creating documents using XML is to give structure and meaning to documents, rather than continuing to create unstructured information.

If documents are created using XML in a standard way — for example, in accordance with the RDF — then software agents can retrieve the information in a standard way. The impact for litigators is that devices can be located by their internet addresses; information can be collected and analysed; and searches can be undertaken using sophisticated search tools and clustering, using metadata that has been pulled directly from the documents. Software can be developed to recognise markup in XML documents, and simplify the retrieval process.

The internet of the future will, as it has done in the past, continue to make our lives easier; the trick is to make it work for us in ways to ensure that information retrieval continues to be simpler. The key will be in the creation of structured information in accordance with Sir Tim Berners-Lee's vision for the future. ●

Allison Stanfield, Executive Director, e.Law Australia Pty Ltd.

Endnotes

1. *Seven Network Ltd v News Ltd* [2007] FCA 1062 BC200705841.
2. Merritt C 'E-documents to slash expense of case paper chase' *The Australian* 27 July 2007 p 29.
3. Above note 1 at [1].
4. Above at [1.1.1].
5. Above note 2.
6. Van Beijnum I 'Everything you need to know about IPv6' (7 March 2007) at <http://arstechnica.com/articles/paedia/IPv6.ars>.
7. Above.
8. Huston G 'IPv6 — evolution or revolution' Internet Society (January 2006) at <www.potaroo.net/papers/isoc/2006-01/ipv6revolution.html>.
9. Hinden R M 'IP next generation overview' (14 May 1995) at <http://playground.sun.com/ipv6/INET-IPng-Paper.html>.
10. Above.
11. [2002] VSC 73 BC200201564.
12. *British American Tobacco Australia Services Ltd v McCabe* (2002) 7 VR 524.

Succeeding in e-negotiations

Benedict Sheehy UNIVERSITY OF NEWCASTLE, AUSTRALIA and
Norbert Palanovics NAGOYA UNIVERSITY, JAPAN

Introduction: the changing medium of decision making

All types of negotiations, including many negotiations by lawyers, are now just as likely to be done by email as face-to-face. It is critical, therefore, that research address this changed manner of negotiation, because the medium can affect significantly not only the negotiating process,[1] but the outcome as well.[2] We know that email negotiations tend to break down more easily, and we thought it would be worthwhile to investigate why — and what, if anything, could be done to improve the situation. In order to answer these questions, we conducted an empirical study which we report on in summary form here.

Negotiation theory

Negotiation can be defined as the resolution of conflicting interests by seeking mutually acceptable solutions. There are two main approaches to negotiation. One approach is a broader, more inclusive approach, called integrative negotiation, and the other, which focuses on maximising individual gain, is called distributive negotiation. The general consensus is that the two approaches to negotiation do not produce the same quality of resolution.[3] Furthermore, it is generally agreed that in many situations the most effective negotiated resolutions are those that include an integrative element.[4] Integrative negotiation, or 'win–win' negotiation, is a model of negotiation that requires a collaborative approach. It looks to solve the problems of both parties by addressing each party's needs[5] and focuses on mutual gain instead of maximising individual benefits without regard to the costs of the other party. Integrative negotiation permits the parties to make optimal utility of all resources, rather than limiting the negotiated solution to distribution of the obvious resources at hand.

Although integrative negotiation is usually considered to result in superior, integrative outcomes, for various reasons it is not the usual or most commonly used model.[6] The most commonly used model is distributive negotiation, in which the parties focus exclusively on dividing resources. The situation is viewed as zero–sum — any gain by one party is necessarily an equal loss to the other. To achieve integrative negotiation, a non-zero–sum or non-distributive approach needs to be developed, and a basic level of trust must be developed, discussed in the literature as 'intangibles' or 'relationship'.[7]

For any negotiation to occur, there must be some type of relationship. A relationship signifies a certain level of communication and trust. Yet communication and trust cannot be the only rule, as any negotiation requires careful management of the disclosure, discovery and concealment of information. Concealed information and the risk of loss in the distributive aspect of negotiation create a basis for a 'danger' or stress response. This stress response may have, among other things, an impact on negative attribution.[8] How the stress response is identified and managed, we believe, will have a significant effect on the negotiation.

Computer mediated communication — email

Negotiation via computer is computer mediated communication (CMC). Email is one type of CMC. It is multi- or bidirectional — it can have more than one recipient — and it is low-cost and high-speed.[9] Its contents can include all types of data, including images and video. Being asynchronous, the negotiating parties likely do not share the same environment; are not able to see what the other is doing; and read and reply to the email at a time and location most convenient to each individual. Interaction is only via computer, usually in an isolated environment such as a solitary person in an office.[10] Email's lack of non-verbal feedback has a deleterious effect on communication. When people are deprived of feedback, they rely on their own intuition, or their imagination.[11]

Email's lack of non-verbal feedback has a deleterious effect on communication. When people are deprived of feedback, they rely on their own intuition, or their imagination.

Email, relationship building and negotiations

The lack of social cues in email and the effects of this lack on relationship building have been the bases of various studies on email negotiations. Researchers Thompson and Nadler have found that when parties share social ties or 'schmooze' — that is, build interpersonal relationships and engage in non-task-related activities — their chances of obtaining a good

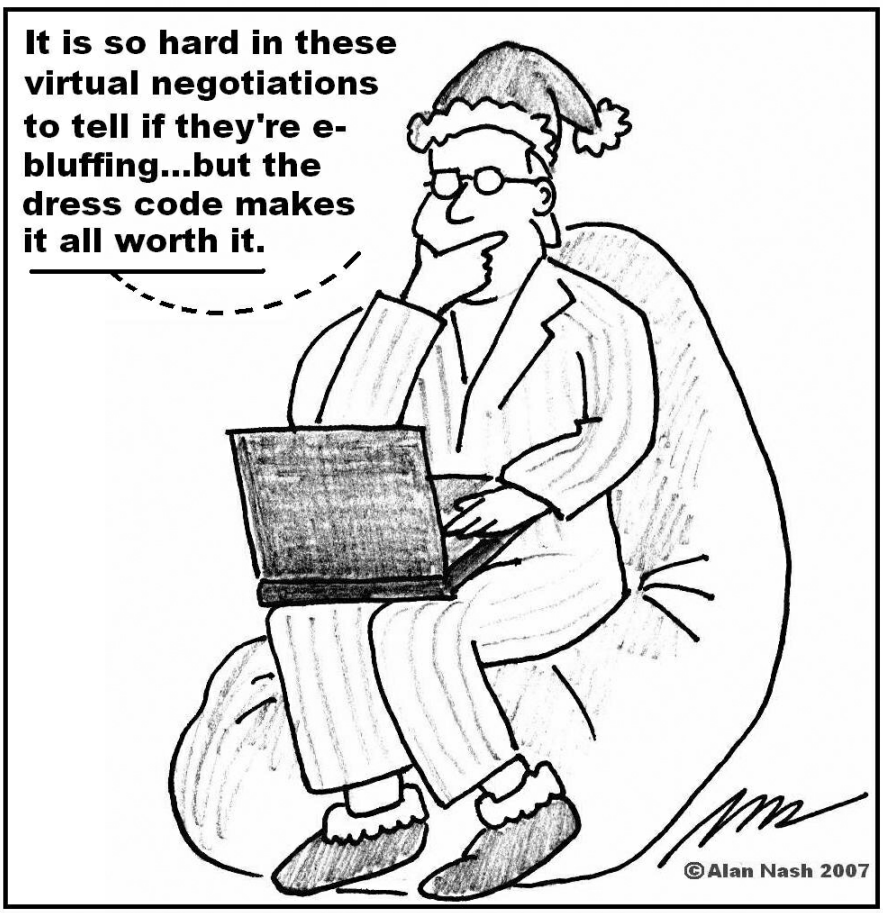
agreement are increased.[12] The importance of shared social ties, or 'shared membership', is also stressed by Moore, Kurzberg, Thompson and Morris, who found that when there is shared membership between negotiators, email negotiations can be as integrative as face-to-face negotiations.[13] Probably the biggest challenge of email negotiation is to establish a relationship that includes trust.[14] In our study, we focused on the variables of rapport building and reducing anonymity as two aspects of the broader category of 'relationship', and the variable of attribution of intention as a sub-category of the larger issue of trust.

The current study

Rapport refers to a higher level of comfort in communicating with another person — that is, one has confidence that the other party has a high probability of understanding, as well as confidence that if a misunderstanding occurs, it will not be difficult to correct. Normally, rapport is developed through small talk. The second variable studied is reducing anonymity — the sense of being unknown — as it lowers one's sense of responsibility and accountability to others.[15] As a result, it lowers one's social inhibitions in comparison to when one is operating as an individual and as known to a community.

The third variable, attribution of intention, addresses one aspect of the issue identified as decoding.[16] When we receive messages, part of the interpretive framework is made up of our understanding of what the other person intends. Attribution is addressed both in the psychological literature[17] and in the cross-disciplinary study of hermeneutics.[18] In each case, the importance of the receiver–interpreter's idea of the sending party's intentions is critical in the reception and interpretation that the message will receive.

Attribution is an individual activity and depends to a large degree on the mental and emotional state, and the general psychological disposition, of the individual.[19] Nevertheless, we have assumed that it is possible in a controlled, time-limited condition to have an influence on this general disposition in a particular situation.



Experiment

We decided to test our ideas via an experiment with a group of undergraduates who were studying negotiations but were unknown to each other. We hypothesised that if certain activities could be used to address these three variables, outcomes of a problem negotiated by email would be improved. Accordingly, in our study we developed instructions to create an opportunity for rapport building, such as exchanging information about personal likes and dislikes. Also, we instructed the parties to use each other's names in the negotiation and exchange photos to reduce anonymity. Finally, we instructed the parties to address their negative attributions of intention by thinking about them and writing them down. We designed an experiment in which the students negotiated a problem without any instructions specific to email negotiations, and a subsequent negotiation after being giving instructions. After each of the two sets of negotiations, both the processes and the outcomes were analysed.

Findings and conclusion

We found that the instructions worked to improve both the number of agreements and the number of integrative agreements. We found that rapport building improved the number and integrative quality of the agreements achieved. One way in which lawyers often build rapport is to ask such things as what law schools they have attended, or see if there are other senior lawyers known by both. Lawyers may also discuss cases they have worked on, favourite judges, or opinions on legislative changes or court systems. We would suggest, therefore, that exchange of non-task-related information would likely result in improved negotiated outcomes. In other words, by spending some time on small talk, the outcomes of the negotiation in terms of satisfaction and likelihood of achieving an agreement in general would be improved.

Although we hypothesised that reduced anonymity would improve the process, from our research we concluded that although providing instructions contributed to a reduction in anonymity, it did not have an effect either on the number of agreements or on the integrativeness of the negotiations. Our third hypothesis, that being aware of the attributions of intention should increase the integrated outcomes as well as the number of agreements, was borne out by the research. Indeed, one of the main factors affecting integrativeness is the attribution of intention. It will be important for lawyers to consider the intentions they attribute to the other party. That party is not necessarily looking for every opportunity to take advantage of the situation or necessarily looking to use every available strategy to advance his or her position at the expense of the lawyer's client. Accordingly, an appropriate strategy will require the lawyer to consider carefully his or her own thoughts on the matter and possibly to write them down to develop a considered response to the negotiation as it unfolds through email. ●

In other words, by spending some time on small talk, the outcomes of the negotiation in terms of satisfaction and likelihood of achieving an agreement in general would be improved.

Benedict Sheehy, Lecturer, School of Law, University of Newcastle, Australia, and
Norbert Palanovics, Researcher, Nagoya University, Japan.

Endnotes

1. McGinn K L and Croson R 'What do communication media mean for negotiations? A question of social awareness' in Gelfand M and Brett J (eds) *Culture and Negotiations: Integrative Approaches to Theory and Research* Stanford University Press 2003.
2. Valley K L, Moag J and Bazerman M H 'A matter of trust: affects of communication on the efficiency and distribution outcomes' (1998) 34 *Journal of Economic Behavior & Organization* 211–38.
3. Lewicki R J, Saunders D M and Barry B *Negotiation* (5th edn) Irwin/McGraw-Hill 2006 p 3.
4. Fisher R, Ury W and Patton B *Getting to Yes: Negotiating Agreement Without Giving In* (2nd edn) Penguin 1991 p 7.
5. Fisher, Ury and Patton, above note 4.
6. Lewicki, Saunders and Barry, above note 3.
7. Fisher, Ury and Patton, above note 4.
8. Seligman M E P *Learned Optimism* Pocket Books 1998 pp 40–43.
9. Kedzie C R 'A brave new world or a new world order?' in Kiesler S (ed) *Culture of the Internet* Erlbaum 1997 pp 209–32.
10. Sproull L and Kiesler S 'Computers, networks and work' (1991) 265 *Scientific American* 116–23.
11. Mehrabian A *Silent Messages: Implicit Communication of Emotions and Attitudes* (2nd edn) Wadsworth 1981.
12. Thompson and Nadler.
13. Moore D A, Kurtzberg T R, Thompson L L and Morris M W 'Long and short routes to success in electronically mediated negotiations: group affiliations and good vibrations' (1999) 77(1) *Organizational Behavior and Human Decision Process* 22–43.
14. Gunderson.
15. Carpenter J 'Endogenous social preferences' (2005) 37 *Review of Radical Political Economics* 63–84.
16. Shannon C E and Weaver W *The Mathematical Theory of Communication* University of Illinois Press 1949.
17. Seligman, above note 8.
18. Gadamer H *Truth and Method* Seabury 1975; Lonergan B *Insight: A Study of Human Understanding* (3rd edn) Philosophical Library 1970.
19. Burns D *Feeling Good: The New Mood Therapy* (revised edn) Avon, New York 2001; Seligman, above note 8.

Employee privacy — the forgotten issue

Patrick Fair and **Ryan Grant**
BAKER & MCKENZIE

Jane is pregnant. A personal email congratulating her is sent to her work email address. The email is read by a network engineer as part of company policy and is forwarded to her manager, who congratulates her in the lunch room. Has anybody broken the law? Most businesses are alive to privacy issues as they relate to customer information, but few have regard to the *Privacy Act 1988* (Cth) (the PA) as it relates to employee information that falls outside the employee record exemption. It this article we survey the state of the law relating to privacy in the workplace.

State workplace surveillance Acts

NSW

The *Workplace Surveillance Act 2005* (NSW) (the WSA) sets out the requirements that an employer must fulfil in order to monitor employees' computer usage (among other things). It does this by prohibiting covert surveillance of employees without authorisation.[1] Unauthorised covert surveillance carries a potential $5500 fine. If employees are given 14 days' notice, pursuant to Pt 2 of the WSA, that specific surveillance will occur, that surveillance is no longer covert.[2] Additionally, for computer surveillance, the surveillance must be carried out in accordance with an employer policy and the employee must be notified such that it would be reasonable to assume the employee is aware of the policy.[3]

The WSA gives little guidance on the principles that are to apply with respect to the collection, use, protection and dissemination of the often large amounts of data produced by employee overt surveillance. Even though the WSA provides restrictions on the disclosure to persons outside the employer's business, there is scant restriction on the flow of the data within the business.

Victoria

In 2005, the Victorian Law Reform Commission made recommendations regarding policies for electronic workplace surveillance, genetic testing in the workplace and drug and alcohol testing in the workplace. To date, the only response has been the *Surveillance Devices (Workplace Privacy) Act 2006* (Vic), which prohibits the placement of video surveillance in change rooms and bathrooms.

WA

The *Surveillance Devices Act 1998* (WA) makes it an offence for employers (or employees) to use, install or maintain listening devices to record a private conversation; optical surveillance devices to record visually or to observe a private activity; and tracking devices to determine the geographical location of a person. There is no provision for restrictions on computer surveillance.

Queensland, SA, Tasmania, the ACT and the NT

These states and territories have no specific workplace surveillance legislation.

The employee record exception to the Privacy Act

The Commonwealth PA broadly regulates the collection of personal information. Personal information is any information that relates to an identified or identifiable individual. If a private organisation collects personal information, it is bound by the National Privacy Principles (NPPs) set by the Privacy Commissioner. There are some exceptions, the most relevant here being the employee record exception.

Section 7B(3) of the PA grants employers exception from the Act in certain circumstances. Three elements must be satisfied for the exception to apply: the organisation must be acting in the capacity of a current or former employer; the dealings with the data must be directly related to that employee/employer relationship; and the dealings with the data must be directly related to that employee's *employee record* held by the employer.

Acting in the capacity of a current or former employer

This requirement means that information collected regarding a prospective employee is excluded from the exception. Additionally, information collected about an employee during the employee's transactions as a customer of the organisation are excluded. These exceptions may not appear all that important; however, it is very common to collect references and perform background checks in addition to collecting CVs and taking notes in interviews for prospective employees. All the data collected in these examples will fall within the scope of the PA.

Related to the employee/employer relationship

If an employer does something with the employee's data that is not related to the employment relationship, the employer is not protected by the employee record exception. In practice, an employer is most likely to fall foul on this exclusion if they use employee data for commercial purposes. For example, because of this requirement, employee information that is sent to an alliance partner as part of the cross-promotion of products in a business alliance will fall outside the 'employee record' definition.

Related to that employee's record held by the employer

This exemption only applies as long as the record is held by the employer. If the information is disclosed to another organisation, such as an insurance company, the exception from the PA no longer applies to the information held by that insurance company.

Additionally, s 6(1) of the PA presents a non-exhaustive list of types of information that are included in the 'employee record'. Information regarding the employee's terms of employment, hours, leave, superannuation and performance are included. The data must relate to the employment relationship. With this in mind, it is clear that private emails or web-browsing data do not relate to the employment relationship and are not part of the employee record. A possible link to the employment relationship is the misuse of these facilities. However, the Federal Privacy Commissioner has expressly stated that logs of staff web-browsing activities are subject to the provisions in the PA.[4]

Importantly, if a person visits certain websites on the employer's equipment, the web-address data recorded may reveal information about their religion, sexual preference, ethnic origin or membership of a union or political organisation. Private emails could also reveal similar information.

Importantly, if a person visits certain websites on the employer's equipment, the web-address data recorded may reveal information about their religion, sexual preference, ethnic origin or membership of a union or political organisation. Private emails could also reveal similar information. As such, a person's web and email usage data could easily contain information that is defined under the PA as 'sensitive information'.[5] Collection of this form of data attracts increased regulation from the PA, which will be examined below.

It seems clear that while much of the information collected by employers is exempt from the PA, there are definite gaps in the protection that employers who conduct electronic surveillance need to be aware of. This is particularly relevant for those employers in states where notification of computer surveillance is not necessary. While some state legislative schemes may not require notification, the PA does. These gaps are relevant when drafting privacy policies and employee computer use policies.

Other sources of privacy rights

Common law breach of confidence may also give rise to actions against an employer. Although not well defined in the area of employment law, the three elements of an action could conceivably be fulfilled in an employment context. The elements that form the tort are that the information disclosed is inherently confidential or expressly stated to be confidential; that it was imparted in circumstances which created an obligation of confidence either expressly or impliedly; and that the employer has threatened or has actually disclosed the information without the employee's authority.[6]

Where the employer collects the information automatically, with the employee's knowledge, there may not be circumstances that impart confidentiality. On the other hand, there may be an expectation that information about private emails and web browsing would be kept confidential when the employee agreed to its collection.

Accordingly, there are two legislative schemes that organisations address in order to avoid liability. First, if you are conducting overt electronic surveillance

of your employees in NSW, you must be aware of the notification obligations under Pt 2 of the WSA and the restrictions regarding what surveillance is acceptable, as provided for by that Act. Second, if the information your organisation is collecting about an employee is not covered by the s 7B(3) (employee record) exception (most relevantly, email and web usage data), the PA and thus the NPPs apply to that information.

NSW Workplace Surveillance Act

Should you wish to conduct surveillance of an employee's computer use in NSW, you must have a detailed policy that is brought to the attention of staff at least 14 days before the surveillance. The policy should be explicit as to what activities are permitted and forbidden; management should ensure that staff members are aware of the policy and its contents; and the policy should set out exactly what information is recorded and who is going to have access to that information.

For the other states and territories, at this stage employees do not have to be notified if the surveillance is limited to computer surveillance.

Commonwealth Privacy Act

Where the data is personal information and is not covered by the employee record exception, the PA applies to the collection and use of that information. The NPPs set out 10 principles that all private organisations must adhere to when collecting personal information. The following is a brief summary of the NPPs:

- the individual must be made aware of who is collecting the data, why the data is being collected, the fact that he or she is able to access that data, and the types of organisations that the employer usually discloses the data to;
- the collection of the information must be necessary for the organisation's activities;
- generally, the information can only be used for its original purpose;
- reasonable steps must be taken to ensure the accuracy and security of the information;
- there must be documentation regarding the organisation's information collection practices;
- individuals must have access and correction rights; and
- there are special provisions for information deemed 'sensitive personal information'.

For information that falls into the last category, the organisation must seek explicit consent from the individual. This may include the production of a comprehensive computer use policy, but the individual must also expressly agree to the collection of data in the manner detailed in the policy, not just be notified of it.

The PA covers all Australian jurisdictions and, as such, a privacy policy regarding the information that falls outside the employee record exception must be created and distributed even if there is no state or territory legislative requirement to do so.

Conclusion

Employers in states and territories that do not have specific computer surveillance legislation can still fall foul of the Commonwealth privacy legislation. Employers in NSW must also be aware of the obligations placed on them by the PA, in addition to the WSA. A privacy policy that merely deals with customer data is not sufficient. A great deal of personal information collected and stored regarding employees should and must be addressed according to the NPPs. ●

Patrick Fair, Partner, and
Ryan Grant, Graduate at Law,
Baker & McKenzie, Sydney.

Endnotes

1. Section 19.
2. Section 3, 'covert surveillance'.
3. Section 12.
4. Office of the Federal Privacy Commission *Guidelines on Workplace E-mail, Web Browsing and Privacy* (30 March 2000) <www.privacy.gov.au/internet/email/index_print.html> (accessed 3 March 2007).
5. Section 6, 'sensitive information'.
6. *Coco v A N Clark (Engineers) Ltd* [1969] RPC 41 at 47.

Geo-location technologies, internet gambling and the law

Dr Dan Jerker B Svantesson BOND UNIVERSITY

The internet is frequently referred to as being 'borderless' — people move around effortlessly from jurisdiction to jurisdiction with little regard to the geographical borders they cross. At the same time, when disputes arise in relation to conduct taking place on this borderless internet, we are reminded of the fact that internet conduct originates in actions taken by physical persons in geographically identifiable real-space locations.

The relevance of geography is also apparent when a government seeks to legislate in relation to internet conduct. For example, geography plays a central role in how Australia regulates internet gambling.

This article examines how so-called geo-location technologies — technical means for ascertaining the geographical location of internet users — fit within the Australian approach to regulating internet gambling.

The Interactive Gambling Act

In 2001, the Australian Government introduced the *Interactive Gambling Act 2001* (Cth) (the Act). The Act fulfils four different functions.

- It prohibits interactive gambling services from being provided to customers in Australia and some other specifically designated countries.[1]
- It establishes a complaints-based system to deal with internet gambling services available for access by customers in Australia and some other specifically designated countries.[2]
- It caters for the development of an industry code.[3]
- It prohibits the advertising of interactive gambling services.[4]

As far as the prohibition of interactive gambling services is concerned, the key provision of the Act is s 15. In subs 1, s 15 states that:

> A person is guilty of an offence if:
> (a) the person intentionally provides an interactive gambling service; and
> (b) the service has an Australian-customer link …

According to s 5(1), an 'interactive gambling service' is a gambling service, where:

> (a) the service is provided in the course of carrying on a business; and
> (b) the service is provided to customers using any of the following:
> (i) an Internet carriage service;
> (ii) any other listed carriage service;
> (iii) a broadcasting service;
> (iv) any other content service;
> (v) a datacasting service.

The definition of 'interactive gambling service' is rather wide. However, it excludes a range of forms of interactive gambling such as traditional telephone betting.[5] Further, due to successful lobbying by certain organisations, the Act draws a distinction between 'gambling' and 'wagering' — the former being regulated and the latter not being regulated. This means that, while activities such as online casinos are regulated, websites providing, for example, sports bets are not.[6]

Section 8 of the Act discusses when a service has an Australian-customer link. It makes clear that 'a gambling service has an Australian-customer link if, and only if, any or all of the customers of the service are physically present in Australia'. This section highlights the importance of the physical location of internet users, and thereby also the importance of geography as such.

Where a provider of an interactive gambling service did not know and could not, with reasonable diligence, have known that the service had such an Australian-customer link, it has not committed an offence under s 15(1). Several factors are taken into account in assessing whether this is the case. Subsection 4 lists the following matters to be taken into account:

> (a) whether prospective customers were informed that Australian law prohibits the provision of the service to customers who are physically present in Australia;
> (b) whether customers were required to enter into contracts that were subject to an express condition that the customer was not to use the service if the customer was physically present in Australia;
> (c) whether the person required customers to provide personal details and, if so, whether those details suggested that the customer was not physically present in Australia;
> (d) whether the person has network data that indicates that customers were physically present outside Australia:
> (i) when the relevant customer account was opened; and
> (ii) throughout the period when the service was provided to the customer;
> (e) any other relevant matters.

Subsections (a), (b) and (c) of this provision suggest that a website operator relying on self-identification — that is, the internet users voluntarily identifying their geographical locations — may be protected under the Act as having taken sufficient steps to avoid an Australian-customer link. If that is correct, this sets the Australian approach apart from how some other countries have approached similar matters.

For example, the US *iCraveTV*[7] case involved a Canadian web company, iCraveTV, which provided real-time TV via the company's website. Being aware that their activities may be unlawful outside Canada, even though they arguably were legal at the time in Canada,[8] iCraveTV relied upon self-identification to exclude non-Canadians from accessing their services. When a person accessed iCraveTV's website, he or she was asked to enter his or her local area code. If this area code was not a

Canadian local area code, the person was refused access. However, as noted by Geist, this step for geographical restriction could be viewed 'as rather gimmicky', as the local area code of Toronto, iCraveTV's place of business, was clearly stated on the site.[9] Having entered a valid Canadian local area code, the person seeking to access the website had to certify being located in Canada by clicking on an 'In Canada' icon in a click-wrap agreement. In the third and last access step, the access seekers had to click 'I agree' on another click-wrap agreement, containing the full terms of use (including a verification of being located in Canada).

Despite these steps to ensure an exclusive Canadian group of users, a US court claimed jurisdiction over iCraveTV, which was sued by a group of broadcasters, movie studios and sports leagues.[10] Having seen that a US court found itself to have jurisdiction, it is no surprise that the Canadian company lost the case.[11] The *iCraveTV* case illustrates that the value of self-identification is by no means universally accepted.

Even if it is concluded that providers of online gambling services currently are protected where they rely on self-identification, they may still wish to consider implementing technical measures for avoiding an Australian-customer link. The Explanatory Memorandum to the Act highlights that the defendant:

> … must adduce or point to evidence that suggest they did not know that the service had an Australian-customer link and could not, with reasonable diligence, have ascertained that the service had an Australian-customer link.[12]

The Explanatory Memorandum also notes that:

> If the defendant does this then the prosecution would then need to disprove that the defendant did not know, and could not with reasonable care and diligence have ascertained, that the service had an Australian-customer link.[13]

Further, the Explanatory Memorandum states that:

> In determining whether the use of geolocation software programs or other monitoring systems constituted reasonable diligence, regard would need to be had, amongst other things, to the technical and commercial feasibility of using such programs or systems.[14]

This statement was presumably intended to provide some guidance as to whether a defendant, having relied upon geo-location technologies, can be seen to have acted reasonably to ascertain possible Australian-customer links. However, it could also be looked at from the opposite perspective — that is, can a defendant who has not used geo-location technologies be seen to have acted reasonably to ascertain possible Australian-customer links?

The review of the operation of the Act presented in July 2004 noted that:

> … the provision of network data from the use of geolocation is only one of a number of factors that are to be taken into account in determining whether an IGSP [Interactive Gambling service Provider] had used reasonable diligence to ascertain whether their service had an Australian-customer link.[15]

However, bearing in mind that there is a wide range of geo-location products on the market,[16] it may very well be the case that we now have reached a point in time where it is no longer viable to argue that a defendant could not, with reasonable diligence, have ascertained that its service had an Australian-customer link, if it has not applied a geo-location technology in order to ascertain any such link.

Geo-location technologies

As discussed, there are both technological and non-technological methods enabling website operators to identify the geographical location of those who visit their websites. Self-identification, in its various forms, is a non-technological method, and geo-location technologies are examples of technological methods. Further, the level of sophistication of the different technological methods varies. The most sophisticated methods translate IP addresses[17] into geographical locations by the use of information stored by the provider of the geo-location service.

So how do sophisticated geo-location technologies work? As a person enters the appropriate Uniform Resource Locator (URL)[18] into his or her browser, or clicks on the appropriate hyperlink, an access request is sent to the server operating the requested website. As the server receives the access request, it, in turn, sends a location request (for example, forwards the access seeker's internet Protocol (IP) address[19]) to the provider of the geo-location service. The provider of the geo-location service has gathered information about the IP addresses in use and built up a database of geo-location information.[20] Based on the information in this database, the provider of the geo-location service gives the website server an educated guess as to the access seeker's location (in some cases down to city level). Taking account of this information, the web server can provide the access seeker with the information deemed suitable (for example, a message along the lines of: 'This website may not be accessed by people in Australia').

The accuracy of these products has been the object of debate. While the providers indicate the potential accuracy to be very high, 'over 99% at a country level and approximately 92% at a city-level',[21] they are after all trying to sell a product, and these impressive figures have been criticised.[22] There is a range of factors affecting the accuracy of geo-location technologies. Due to the dual nature of the geo-location process, these factors can be divided into two categories: 'source problems' and 'circumvention problems'.

The source problems are the problems associated with building up and/or collecting accurate geo-location data. In relation to IP addresses, there is no real equivalent to the address registers listing physical addresses, or the phone registers listing phone numbers — at least not currently. Consequently, the ones creating databases of geo-location information must rely on other, less straightforward, methods. Obviously, the accuracy of the material in the geo-location databases depends on, and can never be better than, the accuracy of the collection of that data. Common methods of collecting relevant material include, for example, gathering data from registration databases,[23] network

routing information, DNS systems, host name translations, ISP information and web content.[24] All of these sources may provide inaccurate information.[25]

Turning to circumvention problems, it can be noted that while some circumvention techniques are technologically advanced (for example, deep linking to streaming video content without accessing the HTTP server[26]), others are easy enough to be used by virtually anyone (for example, anonymising techniques[27]) or even inherent in the system structure ('tunnelling methods'[28]). With this in mind, people with sufficient skill and motivation will presumably always be able to circumvent geo-location technologies.

Concluding remarks

It is clear that geo-location technologies have several benefits. As discussed, such technologies can, for example, be used to limit the geographical distribution of content, thereby ensuring regulatory compliance. Other benefits include fraud detection, spam minimisation and content targeting (for example, geographically targeted advertisement). However, at the same time, the use of geo-location technologies has at least one major negative consequence — it has the potential to destroy the internet's 'borderlessness'. The ability to communicate freely across borders is doubtlessly one of the key ingredients in the internet's enormous success, and the use of geo-location technologies works against this — geo-location technologies place borders on the borderless internet, thereby making it more similar to the physical world divided by borders of various kinds.

Thus, the conclusions that can be drawn from the above are twofold:

- geo-location technologies support the approach to geography taken in the Australian Act; and
- the approach to geography taken in the Act encourages the use of technologies that have the potential to destroy one of the internet's most fundamental characteristics. ●

Dr. Dan Jerker B Svantesson,
Assistant Professor,
Faculty of Law, Bond University,
Gold Coast, Queensland.

This article partly draws upon Dr Svantesson's article 'Geo-location technologies and other means of placing borders on the "borderless" internet' (Fall 2004) 23(1) John Marshall Journal of Computer & Information Law *101–39.*

Endnotes

1. Parts 2 and 2A.
2. Parts 3–7.
3. Part 4.
4. Part 7A.
5. Section 5(3).
6. See, for example, ss 5(3), 8A and 8D.
7. *Twentieth Century Fox Film Corporation et al v iCraveTV et al* 2000 US Dist LEXIS 11670; 53 USPQ2D (BNA) 1831 (8 February 2000).
8. Under Canadian law, as it then stood, internet retransmission of over-the-air television was allowed under certain conditions and provided that the retransmission was for Canadians only. The important aspect of this is, of course, that no copyright restrictions were attached to the retransmission. However, a change (Bill C-11, adopted in 2002) to s 31 of the *Copyright Act* (CA) created an 'internet carve-out' in relation to the compulsory licence regime. See further Broadcasting Public Notice CRTC 2003–02 (Ottawa, 17 January 2003). For a detailed discussion of the legality of iCraveTV's operation, see Geist M 'iCraveTV and the new rules of internet broadcasting' (2002) 23 *University of Arkansas at Little Rock Law Review* 223–42.
9. Geist M 'Is there a there there? Towards greater certainty for internet jurisdiction' (2001) 16 *Berkeley Technology Law Journal* 1345, at 6 (stated page number refers to PDF version, available at <http://aix1.uottawa.ca/~geist/geistjurisdiction-us.pdf> (accessed 17 May 2007)). On the other hand, for a company to state its physical address on the website could be seen to be good practice, and indeed is required, for example, under European Community law. See Directive 2000/31/EC on electronic commerce, Art 5(1b-d). It should also be mentioned that efforts along these lines have been made on several levels. See, for example, the OECD's work in relation to the accuracy of 'WHOIS' data: 'Consumer policy considerations on the importance of accurate and available WHOIS data' (June 2003) at <www.olis.oecd.org/olis/2003doc.nsf/LinkTo/dsti-cp(2003)1-final> (accessed 17 May 2007).
10. 'iCraveTV is served up a lawsuit' *Wired News* 20 January 2000 at <www.wired.com/news/business/0,1367,33797,00.html> (accessed 17 May 2007); Geist M, above note 9 at 5.
11. Above note 7.
12. Explanatory Memorandum to the Act at 54.
13. Above.
14. Above.
15. Department of Communications, Information Technology and the Arts *Review of the Operation of the 'Interactive Gambling Act 2001'* (July 2004) at 73.
16. See, for example, <www.quova.com> (accessed 17 May 2007); <www.akamai.com> (accessed 17 May 2007); and <www.digitalenvoy.net/> (accessed 17 May 2007). See also the following geo-location products that can be tested for free online: <www.activetarget.com/livedemo.asp> (accessed 17 May 2007); <www.ip2location.com/free.asp> (accessed 17 May 2007); and <www.geobytes.com/IpLocator.htm> (accessed 17 May 2007).
17. There are currently approximately 1.3–1.6 billion IP addresses in use, out of the 4.25 billion possible addresses that can be issued under the four-block range from 0 to 255. See further van Leeuwen A 'Geo-targeting on IP address: pinpointing geolocation of internet users' (July/August 2001) *Geo Informatics*; Olsen S 'Geographic tracking raises opportunities, fears' *CNET News.com* 8 November 2000; and Spangler T 'They Know — roughly — where you live' *eWEEK* 20 August 2001.
18. '[URL], Abbreviation of Uniform Resource Locator, the global address of documents and other resources on the World Wide Web. The first part of the address indicates what protocol to use, and the second part specifies the IP address or the domain name where the resource is located' at <www.webopedia.com/TERM/U/URL.html> (accessed 17 May 2007). For more details, see,

for example, Chappell L A and Tittel E *Guide to TCP/IP* Thomson Course Technology, Boston 2002 p 271.

19. See further <http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci212381,00.html> (accessed 17 May 2007).

20. The methods of collecting this information are discussed below.

21. Digital Envoy product sheet (on file with the author).

22. See, for example, Information Technology Association of America 'Ecommerce taxation and the limitations of geolocation tools' at <www.itaa.org/taxfinance/docs/geolocationpaper.pdf> (5 February 2007) at 6.

23. That is, Réseaux IP Européens Network Coordination Centre at <www.ripe.net> (accessed 7 May 2007); American Registry for Internet Numbers at <www.arin.net> (accessed 17 May 2007); Asia Pacific Network Information Centre at <www.apnic.net> (accessed 17 May 2007); and Latin American and Caribbean IP Address Regional Registry at <http://lacnic.net> (accessed 17 May 2007).

24. See, for example, *Internet Geography Guide — A NetGeo White Paper,* which can be requested from <www.netgeo.com> (accessed 17 May 2007).

25. Edelman B 'Shortcomings and challenges in the restriction of internet retransmissions of over-the-air television content to Canadian internet users' at <http://cyber.law.harvard.edu/people/edelman/pubs/jump-091701.pdf> (accessed 17 May 2007) at 3–7.

26. Above at 10.

27. Above at 8. For some examples of free anonymising services, see <www.svantesson.org> (accessed 17 May 2007).

28. Edelman, above note 25 at 9.

bytes

ICANN'S plans to expand the generic domain name space

The Internet Corporation for Assigned Names and Numbers (ICANN) has announced its plans to expand the domain name system (DNS) by introducing new generic top-level domains (gTLDs) in 2008. ICANN is currently seeking input from businesses, governments and the public at large on the development of a new process for evaluating and approving new gTLDs. The introduction of new gTLDs will effectively expand the internet space and provide registrants or end users with greater choice about the nature of their presence on the internet.

There are currently 16 gTLDs in existence (including the original gTLDs: .com, .net and .org), each of which was created for a general category of organisations. ICANN has been working on the introduction of new top-level domains (TLDs) since 1999.[1] The first expansion of the generic domain name space occurred in November 2000, when ICANN's board of directors selected a first group of new gTLDs: .aero, .biz, .coop, .info, .museum, .name and .pro.[2] In 2004, ICANN directed the second round of expansion of gTLDs with the introduction of six new gTLDs: .asia, .cat, .jobs, .mobi, .tel and .travel.[3]

New gTLDs have previously been created based on proposals that were submitted to ICANN during particular application rounds.[4] Applications which were received during these rounds were evaluated in accordance with previously published criteria, and successful applicants subsequently proceeded with signing TLD Registry Agreements.[5]

ICANN has proposed that the new process in respect of the third round of expansion will outline how gTLDs are proposed and approved, and provide for a much broader variety of gTLDs to be introduced in a timely, predictable and efficient way.[6] ICANN's Generic Names Supporting Organisation (GNSO), which is responsible for creating policy applicable to gTLDS, is currently steering the policy development process and its work will be used as the foundation for discussion on creating a new approval process.[7] Once this policy development process is finalised and a policy has been adopted, ICANN will be able to establish a new gTLD application process.

ICANN anticipates that the system of approving new gTLDs will be finalised by the end of 2007, with applications for new gTLDs being accepted in early 2008.[8] The internet community could expect to see new gTLDs being introduced and available between June and August 2008.[9]

Jaime Riffel, Lawyer, Maddocks Lawyers, Sydney.

ICANN publishes Internationalised Domain Names glossary

On 2 May 2007, ICANN published a glossary of terms relating to Internationalised Domain Names (the IDN glossary). The IDN glossary explains the meaning of terms such as 'Unicode' and 'Punycode' and acronyms such as 'DNS', which represents 'Domain Name System'.

ICANN's creation of the IDN glossary follows the increased demand for multilingual domain names, which has been generated by the widespread use of the internet among diverse linguistic groups in various regions. The IDN glossary aims to provide consistency in IDN-related discussions by encouraging the free use of glossary terms in communications associated with internationalising the domain name space. ICANN expects that the IDN glossary will be expanded over time.

The IDN glossary can be accessed at the ICANN website at <www.icann.org>.

Duncan Giles, Special Counsel, and Howard Cheung, Solicitor, Freehills, Sydney.

ACCC alleges breach of Trade Practices Act by website registrant

On 30 April 2007, the Australian Competition and Consumer Commission (ACCC) instituted legal proceedings in the Federal Court against an internet tobacco website registrant for alleged contraventions of the *Trade Practices Act 1974* (Cth) (the Act).

The ACCC has alleged that the registrant of <www.cheapcigarettes.com.au>, Mr Mina Guirguis, supplied, in his own right or as an agent, cartons of cigarettes that did not include the warning, explanatory and information messages and graphic images mandated by the *Trade Practices (Consumer Product Information Standards) (Tobacco) Regulations 2004* (Cth) (the Regulations).

The ACCC has also alleged that the statement 'There is no refund for our products', displayed on the website from 4 February 2005 to 6 December 2006, was misleading consumers about their refund rights, in breach of the Act.

The ACCC is seeking the following remedies:

- an injunction restraining the registrant from supplying or acting as an accessory to the supply of tobacco products that do not include the requisite warning, explanatory and information messages and graphic images under the Regulations;
- declarations of contravention of the Act;
- a publication order; and
- costs.

At the directions hearing, Mr Guirguis undertook not to supply those cigarettes without the required warning labels until the hearing and determination of the matter. The proceeding was referred to mediation, to be conducted on 15 June 2007.

Duncan Giles, Special Counsel, and Howard Cheung, Solicitor, Freehills, Sydney.

.au domain name policy under review

.au Domain Administration Limited (auDA), the self-regulatory body for .au domain names, is conducting a public review of some key domain name policies. Details can be found at <www.auda.org.au>.

The three policy issues under review are:

- whether domain names should be able to be directly registered at the .au level — for example, lexisnexis.au;
- whether any of the eligibility rules for .com.au, .net.au, .org.au, .asn.au and .id.au domain names should be changed; and
- whether the prohibition on the sale of .au domain names should be lifted.

Public submissions on auDA's issues paper were received by 15 June 2007. After reviewing those submissions, auDA will release its draft recommendations for public comment and then finalise its recommendations for presentation to the auDA board.

Direct registration of .au domain names

Australia has never permitted direct registration of domain names at the .au level, although a number of other countries do permit this — for example, Canada and Japan. Arguments for opening up the .au level for direct registration include that Australia would then have simpler and easier to remember domain names available.

The majority of public submissions oppose this change, arguing that it will result in considerable confusion, both in the allocation of those domain names and in the situation where different traders end up with the corresponding .com.au and .au domain names.

Eligibility rules

There have been fewer submissions on whether the current eligibility rules are too restrictive or too loose. auDA has specifically identified as an issue for consideration whether a policy rule should be included to deal with 'illegal or malicious use of a domain name'.

Sale of .au domain names

Submissions have been more evenly divided on whether or not the prohibition on the direct sale of .au domain names should be lifted. Current policy limits the transfer of .au domain names to transfers falling within certain scenarios — for example, the sale of a business.

On the one hand, many think that the sale of .au domain names often happens in practice and that the transfer of a .au domain name to someone who places a higher value on it because they are able to put it to more effective use should be encouraged.

On the other hand, many think that removal of the prohibition will increase the level of domain name speculation — that is, encouraging people to register a portfolio of .au domain names that they don't intend to use themselves for the sole purpose of on-selling the domain name licences at a premium. This would in turn create an impediment for Australian businesses and organisations wishing to create a new online presence. ●

Craig Smith, Senior Associate, Freehills, Sydney.

Endnotes

1. Generic Names Supporting Organisation *GNSO New TLDs Committee: Draft Final Report — Introduction of New Generic Top-Level Domains* (16 March 2007) at <http://gnso.icann.org/drafts/pdp-dec05-draft-fr.htm>.
2. ICANN *Evaluation of the New gTLDs: Policy and Legal Issues* (prepared for ICANN by Summit Strategies International, 10 July 2004) at <www.icann.org/topics/gtld-strategy-area.html>.
3. ICANN 'Have your say on new top-level domains' (10 May 2007) at <www.icann.org/announcements/announcement-10may07.htm>.
4. ICANN 'New gTLDs — frequently asked questions' (8 May 2007) at <icann.org/topics/new-gtld-strategy-faq.htm>.
5. Above.
6. ICANN, above note 3.
7. ICANN, above note 3.
8. ICANN, above note 3.
9. ICANN, above note 3.

New in paperback (book review)

Yee Fen Lim
Cyberspace Law: Commentaries and Materials

Oxford University Press, Melbourne 2007 (2nd edn)
ISBN: 978 019 5558616; 752 pages (paperback)

The second edition of Yee Fen Lim's *Cyberspace Law: Commentaries and Materials* was released earlier this year.

Having been described as one of Australia's leading texts on internet law, this textbook, primarily targeted at undergraduate and postgraduate students, is well researched and well presented, making it a suitable reference point for lawyers as well.

The book has been comprehensively updated since the first edition, which was published in 2002, and covers the latest developments in all areas of internet law.

Like the first edition, the second edition incorporates key materials from areas including the US, the EU, Singapore and Australia. It also contains new sections on workplace privacy laws, as well as intensive coverage of legislative changes at the Commonwealth level on issues relating to crime in cyberspace, including cyber terrorism. The chapter on electronic signatures includes detailed current developments on digital signatures, with specific focus on updates of the implementation of Public Key Infrastructure systems in strategic jurisdictions.

The chapter on copyright is fully updated and includes the exploration of numerous cases on the concept of secondary liability for copyright infringement in the US and Australia, taking in the P2P cases. Similarly, the chapter on trade marks is packed with new case law developments encompassing the areas of adware and pop-up advertising; sale of keywords or search term associations by search engines; trade marks and domain names; and the use of trade marks on the internet for advertising. Recent litigation in the area of software patents also occupies substantial space in the chapter concerning patents.

Significantly, this second edition boasts fascinating materials on Massively Multiplayer Online Role-Playing Games, a craze which has swept across the world. The new chapters on internet taxation and uninvited materials also provide much food for thought in the expansive reach of internet law.

In the words of the Hon Mr Justice WMC Gummow, as stated in the foreword:

> … this book … will assist all lawyers, whether they be judges, legal practitioners, law teachers or students at law, in coming to grips with a vast range of issues generated by the creation of the internet and the development of what is now called cyberspace.

Yee Fen Lim is on the editorial board of the *Internet Law Bulletin* and has recently joined Galexia in the role of senior consultant, specialising in all areas of e-commerce and IT law. ●

Sharon Givoni, General Editor.

MANAGING EDITOR: Bruce Mills PRODUCTION: Christian Harimanow
SUBSCRIPTION INCLUDES: 10 issues per year plus binder SYDNEY OFFICE: Locked Bag 2222, Chatswood Delivery Centre NSW 2067 Australia
TELEPHONE: (02) 9422 2222 FACSIMILE: (02) 9422 2404 DX 29590 Chatswood www.lexisnexis.com.au bridget.brooklyn@lexisnexis.com.au

ISSN 1329-9735 Print Post Approved PP 244371/00049 Cite as (2007) 10(4) & (5) *INTLB*