ADLSI
Independent Voice of Law

LAWNEWS THIS ISSUE:

Welcome to our special "Technology & Law" edition put together by ADLSI's Technology & Law Committee. We hope you enjoy it!

LAWNEWS

SPECIAL ISSUE TECHNOLOGY & LAW

ISSUE 27 14 AUGUST 2015

www.adls.org.nz

+ Social media and the law, privacy law

CAREFUL WHAT YOU WISH FOR – SOCIAL MEDIA IN THE WAKE OF *HAMMOND v CREDIT UNION BAYWIDE*

By Daimhin Warner, Customer Governance & Privacy Manager, Sovereign

On 2 March 2015, the Human Rights Review Tribunal delivered its decision in *Hammond v Credit Union Baywide* [2015] NZHRRT 6. In doing so, it set a new benchmark for *Privacy Act* litigation and a timely reminder to agencies considering the great green fields of possibilities presented by social media.

The story is a good one and it has now been told countless times. Ms Hammond, a disgruntled ex-employee, posted a photograph of a cake emblazoned with obscenities about Baywide on her Facebook page. She was confident this was safe, as her privacy settings meant only her friends, all 150 of them, could see it. Baywide, however, went to great lengths to obtain the photograph and chose to share it in an attempt to discredit Ms Hammond and ensure that she was unable to secure future employment.

A mark in the sand

It is all too easy to dismiss this case as distinguished by its extreme facts; the Tribunal made no attempt to hide its distaste for the behaviour of the defendant in this case. To do so, however, ignores the guidance this decision provides to us all when considering privacy in this connected world.

The Tribunal has established – albeit with little discussion – that the information privacy principles apply equally in the social media context. It has reinforced the value of social media privacy settings and has upheld the Facebook user's reasonable expectation of privacy, regardless of their desire to share. Finally, the Tribunal has set a new precedent in the award of damages for emotional harm resulting from a privacy breach.

The privacy principles apply

The Tribunal stated simply at the outset that, while this was the first time it had been required to consider the operation of the *Privacy Act* in the social media context, the application of the principles was a simple exercise (para [7]).

Unfortunately, the Tribunal went no further, noting (at para [129]) that "the facts [did] not call for observations to be made about the application of [the privacy] principles in the context of social networking sites." This was a shame, and it ignored a number of interesting questions that, in this writer's view, warranted some thought.

Can someone really argue that personal information they choose to share with over 150 individuals is truly private? While the *Privacy Act* does not require an individual to establish

Continued on page 2

+ Social media and the law, privacy law

CAREFUL WHAT YOU WISH FOR – SOCIAL MEDIA IN THE WAKE OF *HAMMOND v CREDIT UNION BAYWIDE*

Continued from page 1

a reasonable expectation of privacy, as in the common law (see for example *Hosking v Runting* [2004] NZCA 34), it could at least be argued that the decision to share personal information to a wide audience might somewhat reduce the harm that can be claimed as a result of that information then falling into unintended hands.

The answer to this is likely to be the concept of control. The *Privacy Act* recognises that an individual should be able to control what personal information they share with whom. So, by choosing to share personal information with 150 friends, an individual cannot be implied to have consented to sharing it further.

What relevance, then, should one's choice of friends have? As it transpired, in this case at least one of Ms Hammond's friends was a current Baywide employee. In fact, it was through this friend that Baywide obtained the photograph. Could it be argued, therefore, that Ms Hammond knowingly shared her personal information with Baywide? How would the Tribunal's decision have differed had those implicated in the disclosure – the human resources manager for example – been among the 150 friends lawfully in receipt of the image?

As the Employment Court stated in *Hook v Stream Group (NZ) Pty Ltd* [2013] NZEmpC 188 (para [31]), "The reality is that comments made on virtual social networks can readily permeate into real-life networks. Facebook posts have a permanence and potential audience that casual conversations around the water cooler at work or at an after-hours social gathering do not." Does the Facebook user, then, bear some responsibility for the information they share?

The Tribunal also chose not to consider in any depth the application of the collection principles, stating at paragraph 134 that, even if it were to find that Baywide had breached principles 1-4 of the Act, these breaches could not be said to have caused Ms Hammond harm.

This was a pragmatic decision by the Tribunal, recognising that the strongest harm was caused by Baywide's decision to disclose the personal information at issue. However, this decision did somewhat ignore the potential argument that, had the information been lawfully collected by Baywide (and some have argued that principle 2(2) of the *Privacy Act* – that the information was publicly available – may apply), the subsequent disclosure of it may also have been lawful.

Daimhin Warner

The evolution of social media has provided agencies with endless new possibilities to connect with their customers, learn their preferences, speak their language and even predict their desires. However, this valuable and enticing window on the world of the "individual" (be it the employee or the customer) can also represent a major vulnerability and a significant risk. Used well, social media can give a company an edge; make them relevant and connected to the real world. Used wrongly, it can expose companies to a very real and public loss of trust.

Of course, it is relatively clear on the facts that Baywide would have faced a difficult task establishing that its actions had not breached at least principles 2 (source of personal information) and 4 (means of collection of personal information) of the *Privacy Act*. This was an opportunity, however, for the Tribunal to set some precedent in this respect.

Some lessons for the future

Notwithstanding the above, this decision walks new ground for privacy protection in New Zealand, setting a high benchmark for damages awards resulting from a breach of the *Privacy Act*. It provides agencies with a timely reminder to think carefully about the risks they face and the following suggestions are offered to agencies (or their legal counsel) exploring potential uses for social media.

Take a considered approach to the use of social media and think carefully about reputation

The evolution of social media has provided agencies with endless new possibilities to connect with their customers, learn their preferences, speak their language and even predict their desires. However, this valuable and enticing window on the world of the "individual" (be it the employee or the customer) can also represent a major vulnerability and a significant risk. Used well, social media can give a company an edge; make them relevant and connected to the real world. Used wrongly, it can expose companies to a very real and public loss of trust.

Exercise caution in the use of social media to communicate with employees or customers

It is tempting to engage with employees or customers in familiar territory. People enjoy networking online and, as an agency, it may make sense to join them. However, *Hammond v Baywide* should remind us that individual expectations are not always realistic. Perhaps

Continued on page 17

LAWNEWS

LAW NEWS is an official publication of Auckland District Law Society Inc. (ADLSI).

Editor: Lisa Clark

Publisher: Auckland District Law Society Inc.

Editorial and contributor enquiries: Lisa Clark, phone (09) 303 5270 or email lisa.clark@adls.org.nz

Advertising enquiries: Chris Merlini, phone 021 371 302 or email chris@mediacell.co.nz

All mail for the editorial department to: Auckland District Law Society Inc., Level 4, Chancery Chambers, 2 Chancery Street, Auckland 1010. PO Box 58, Shortland Street, DX CP24001, Auckland 1140. www.adls.org.nz

Law News is published weekly (with the exception of a small period over the Christmas holiday break) and is available free of charge to members of ADLSI, and available by subscription to non-members for $130 plus GST per year. If you wish to subscribe please email reception@adls.org.nz

+ *ADLSI Technology & Law Committee*

Introducing the ADLSI Technology & Law Committee in 2015

Innovation lies at the heart of our changing world. From government policy to the practice of law, technology creates amazing opportunities and daunting challenges. The ADLSI Technology & Law Committee (Committee) sees itself as having a mandate to keep up-to-date with the times and offer relevant perspectives on topics such as modernising legal processes, electronic discovery rules, privacy, intellectual property, online safety, cyber-crime and cloud services governance.

The Committee is focused on ensuring, through seminars and articles, that the potential and liabilities of new technology are recognised by the legal profession. In this second annual special "Technology & Law" issue of *Law News*, the Committee continues its focus on providing practitioners with articles and advice on the impact that new technologies are having on law and legal practice.

The Committee has a keen interest in the development of law and policy with a technological aspect. Members maintain a watching brief and make submissions on new pieces of legislation and government policy in relation to the use and security of technology and data security.

Recognising that technology has the potential to impact a whole raft of different legal practice areas, the Committee members bring together a wide range of backgrounds – from the independent bar to law firm practitioners, and from the world of academia to the judiciary – along with diverse practice specialties – ranging from litigation to intellectual property law, relationship property law to franchise law, employment law to criminal law, and regulatory matters to private client and property law.

Current Committee members are:

Melanie Johnson – Heading up the Committee is Committee Convenor Melanie Johnson. Ms Johnson is legal counsel at the University of Auckland. She advises the University primarily on copyright. She has a particular interest in the impact of technology on the way in which copyright material is being generated and used. She can be contacted at mf.johnson@auckland.ac.nz.

Mark Donovan – Mark Donovan is a barrister specialising in employment-related matters and disputes (including mediation, appearances before the Employment Relations Authority and the Employment Court, and advising on employment agreements), as well as acting in relation to other civil disputes (including liquidations, restraints of trade, confidential information and regulatory investigations). He is also the co-founder of Quillo, an online service to help lawyers serve their clients using automated document assembly. He can be contacted at mail@markdonovan.co.nz.

Andrew Easterbrook – Andrew Easterbrook is a senior lawyer at Webb Ross McNab Kilpatrick in Whangarei. He works in the dispute resolution team, dealing mainly with technology law, civil litigation and contentious relationship property disputes. He maintains that zombie law is a legitimate topic worthy of serious discussion. He can be contacted at andrew@wrmk.co.nz.

Lloyd Gallagher – Lloyd Gallagher is actively involved around the world in alternative dispute resolution where he acts as an arbitrator and mediator. With a strong IT background, he works with law practitioners and policy makers to develop solutions that focus on access to justice and technology security. His research focus and consultancy range from technology law, equity, condo disputes, international contracts and tax to regulatory policy through Canada, the UK and Asia Pacific. Mr Gallagher can be contacted at Lloyd@gallagherandco.co.nz.

Kevin Glover – Kevin Glover is a barrister at Shortland Chambers, practising in the area of commercial disputes. He has particular expertise in intellectual property including acting as counsel, teaching at postgraduate level and writing for a number of publications. He writes about intellectual property law and other legal issues on his website, www.iplawyer.co.nz, and can be contacted at kglover@shortlandchambers.co.nz.

His Honour Judge David Harvey – Judge Harvey was appointed as a District Court Judge in 1989, and sat at Manukau for 20 years before transferring to Auckland in 2009. Since his appointment to the bench, Judge Harvey has been closely involved with information technology initiatives involving the judiciary including the development of trial management software.

Arran Hunt – Arran Hunt is a solicitor at Turner Hopkins. Mr Hunt has previously worked as a technical business analyst for a Fortune50 company in London and several large firms and city councils in Auckland, before being admitted in 2010. He has an interest in the interrelation of technology with law and business. He can be contacted at arran@thlaw.co.nz.

Anthony Liew – Anthony Liew is a commercial litigator with a special interest in IP and IT issues. He has practised as a civil litigator in New Zealand and overseas since 1974, following admission as a Barrister of Lincoln's Inn, London. Throughout his career, Mr Liew's main focus has been commercial law, including corporate insolvency and corporate litigation, privacy and terms of trade and intellectual property protection and commercialisation. He can be contacted at aliew@xtra.co.nz.

Edwin Lim – Edwin Lim is a partner at Hudson Gavin Martin, a commercial and corporate law firm specialising in technology and IP. He has specialised in technology, media and intellectual property for over 13 years. With two Honours degrees in Law and Commerce (Management Science and Information Systems), he understands the technical and legal issues involved in a client's project, and is comfortable talking to clients about complex technology matters. He can be contacted at edwin.lim@hgmlegal.com.

Chris Patterson – Chris Patterson joined the independent bar in 2001. He is one of the founding authors of LexisNexis' *Electronic Business and Technology Law*. Since 1997 he has continued to be regularly instructed on matters involving law and technology. He credits one of his greatest, albeit unexplainable achievements, as securing a pass grade in a University computer science paper in 1991. Mr Patterson can be contacted at chris@patterson.co.nz.

Nathan Speir – Nathan Speir is a Senior Solicitor at Rice + Co Lawyers in Auckland. Mr Speir is an experienced courtroom advocate with extensive trial, arbitration and mediation experience. Before joining Rice + Co, Mr Speir commenced his career at the Office of the Crown Solicitor for Auckland where he prosecuted cases on behalf of the Crown and acted for several governmental agencies in a broad range of civil and regulatory matters. He now specialises in local government and insurance litigation and graduated with an LLM (Hons) from the University of Auckland in 2014. Mr Speir can be contacted at nathan@riceandco.co.nz.

Sophie Thoreau – Sophie Thoreau is a Senior Associate with Baldwins Law Limited. Ms Thoreau specialises in the application of intellectual property in commerce, particularly in contentious trade mark and branding-related matters in New Zealand and internationally. She has been involved in a number of complex cases, developing new and emerging concepts of case law for regional and multinational clients of the firm. She can be contacted at sophie.thoreau@baldwins.com.

Daimhin Warner – Daimhin Warner works as Privacy Officer for Sovereign. In this role, he provides operational advice and strategic guidance to the company in respect of the collection, management and disclosure of customer information, including medical information. Prior to this, Mr Warner worked for the Office of the New Zealand Privacy Commissioner for eight years. He has an LLB from Edinburgh University and an LLM in Public Law from the University of Auckland and has been living and working in New Zealand for 13 years. Mr Warner can be contacted at daimhin.warner@sovereign.co.nz.

The Committee welcomes any comments or questions from ADLSI members and other readers amongst the profession. Any correspondence for the Committee should be directed to ADLSI Professional Services Manager and Committee secretary, Helen Young, at helen.young@adls.org.nz.

"Online dispute resolution" for low value claims

By Judge David Harvey

In February 2015, the Civil Justice Councils Online Dispute Resolution Advisory Group, headed by Professor Richard Susskind, produced a report calling for a radical change in the way that the court system of England and Wales handled low value civil claims. The report advocated the introduction of online dispute resolution.

In summary, the basis for such a proposal was that for low value claims of up to £25,000 there were concerns that the current court system was too costly, too slow and too complex, especially for litigants in person. Accordingly, it was recommended that the courts and tribunals service should establish a new Internet based court service known as "HM Online Court" or HMOC.

In this Court, members of the judiciary would decide cases on an online basis, interacting electronically with the parties. Earlier resolutions of disputes on HMOC would be achieved through the work of individuals known as facilitators.

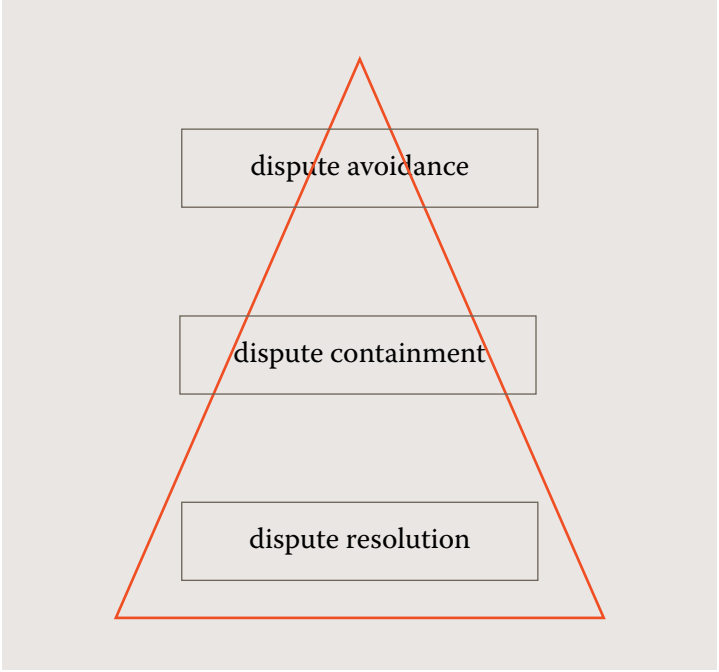
Two major benefits would flow from HMOC – an increase in access to justice in that it would provide a more affordable and user-friendly service, and substantial savings in the costs of the court system. The report emphasised that there were other similar online dispute resolution services – mainly in the area of alternative dispute resolution – which were operating around the world.

One of the important drivers for the online court was that it would involve a system whereby court hearings would be avoided by early efforts to obtain resolution and to contain or isolate the areas of dispute.

The technology underpinning online dispute resolution (ODR) has been evolving rapidly and the report made a number of predictions about the likely capability of later generations of ODR systems.

The report is a broad statement of direction for the future use of ODR. In effect, it paints a "blue sky" picture rather than a detailed one but it envisages technological solutions for online dispute resolution. Furthermore, rather than a focus being upon alternative dispute resolution whereby the parties engage in a private arrangement with a mediator or arbitrator, the service would be provided as part of the established court system.

What is proposed is a multi-tiered system that places emphasis upon dispute identification and resolution rather than, as is the case presently, a court hearing. Professor Susskind depicts the present model in this way:




His Honour Judge David Harvey

The new model is based on these principles:

- affordability – for all citizens, regardless of their means;
- accessibility – especially for citizens with physical disabilities, for whom attendance in court is difficult if not impossible;
- intelligibility – to the non-lawyer, so that citizens can feel comfortable in representing themselves and will be at no disadvantage in doing so;
- appropriateness – for the Internet generation and for an increasingly online society in which so much activity is conducted electronically;
- speed – so that the period of uncertainty of an unresolved problem is minimised;
- consistency – providing some degree of predictability in its decisions;
- trustworthiness – a forum in whose honesty and reliability users can have confidence;
- focus – so that judges are called upon to resolve disputes that genuinely require their experience and knowledge;
- avoidability – with alternative services in place, so that involving a judge is a last resort;
- proportionality – which means that the costs of pursuing a claim are sensible by reference to the amount at issue;
- fairness – affording an opportunity for citizens to present their cases to an impartial expert, delivering outcomes that parties feel are just;
- robustness – underpinned by clear rules of procedure and fully implementing the law of the land; and
- finality – so that court users can get on with their lives.

The report summarises the HMOC approach as follows:

"Tier One of HMOC should provide Online Evaluation. This facility will help users with a grievance to classify and categorise their problem, to be aware of their rights and obligations, and to understand the options and remedies available to them.

"Tier Two of HMOC should provide Online Facilitation. To bring a dispute to a speedy, fair conclusion without the involvement of judges, this service will provide online facilitators. Communicating via the Internet, these individuals will review papers and statements and help parties through mediation and negotiation. They will be supported where necessary, by telephone conferencing facilities. Additionally, there will be some automated negotiation, which are systems that help parties resolve their differences without the intervention of human experts.

"Tier Three of HMOC should provide Online Judges – full-time and part-time members of the Judiciary who will decide suitable cases or parts of cases on an online basis, largely on the basis of papers submitted to them electronically as part of a structured process of online pleading. This process will again be supported, where necessary, by telephone

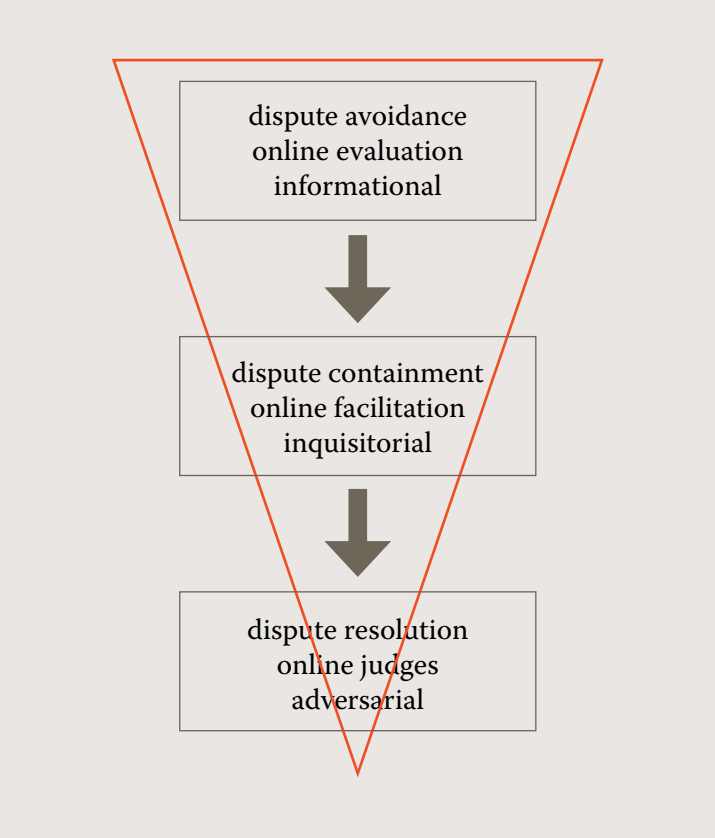
Continued on page 5

Continued from page 4

conferencing facilities.

"The establishment of HMOC will require two major innovations in the justice system of England and Wales. The first is that some judges should be trained and authorized to decide some cases (or aspects of some cases) on an online basis. The second innovation is that the state should formally fund and make available some online facilitation and online evaluation services".

As a result, the diagrammatic representation becomes reversed:



Although the total realisation of the process may be revolutionary in many respects, some of the technologies that underlie the English proposal are currently in place.

Technology is being used for the purposes of communication in many aspects of the court process.

Teleconferencing, particularly of pre-trial conferences or case management conferences, is common.

The *Courts Remote Participation Act 2010* allows for participation by audio visual links. In the criminal jurisdiction, pre-recorded testimony is routine, particularly for vulnerable witnesses.

The provisions of section 103 (and following) of the *Evidence Act 2006* are not limited to criminal procedures.

However, the basis for making orders for giving evidence in an alternative way are somewhat limited pursuant to section 103(3) of that Act.

In most jurisdictions, documents may be filed by email, and although there are no rules authorising filing of commencement documents by email in the District Court or the High Court, it does apply to other documents.

Online dispute resolution is being seriously considered in England.

The English Lord Chancellor, Mr Michael Gove, has spoken positively of the possibilities and potential that this may have there in terms of access to justice as well as savings in the operation of the court process.

The report is available at www.judiciary.gov.uk/reviews/online-dispute-resolution/ and is worthy of consideration. LN

+ Internet law book

internet.law.nz – selected issues, 4th Edition

Author: Judge David Harvey

Pages: 651

Written by Judge David Harvey, the leading authority on the law relating to the internet, the 4th edition of *internet.law.nz – selected issues* is an update on previous editions and contains a range of new material.

Topics examined include speech harms, cyber-bullying and harassment in social and other media, e-discovery and evidence and the impact of the *Search and Surveillance Act*, online defamation and content regulation, the use of information technology in court, and recent developments in internet governance since 2011.

Also included are recent case law and legislation including the Harmful Digital Communications Bill, the *Search and Surveillance Act* and amendments to the *Electronic Transactions Act*.

Price: $147.83 plus GST ($170.00 incl. GST)*

Price for ADLSI Members: $133.04 plus GST ($153.00 incl. GST)*

(+ Postage and packaging)*

To purchase this book, please visit www.adls.org.nz/adlsi-store or contact the ADLSI bookstore by phone: 09 306 5740, fax: 09 306 5741 or email: thestore@adls.org.nz.

The unintended consequences of the *Harmful Digital Communications Act 2015*

By Daniel Gambitsis of the University of Auckland's Equal Justice Project

On 30 June 2015, the *Harmful Digital Communications Act* (HDC Act or Act) passed its third and final reading. The highly controversial Act seeks to "deter, prevent, and mitigate" online bullying and harassment and provide victims with a means of redress.

There is indubitably a crisis of online bullying and harassment in New Zealand. According to *The New Zealand Herald*'s James Ihaka, one in three children in New Zealand has been bullied online. This phenomenon is not limited to children, as shown by the furore created by the "Roast Busters" case and the suicide of New Zealand-born model and TV personality Charlotte Dawson last year, due (at least in part) to persistent harassment by online bullying.

The Act's reception has been far from unanimous, however, owing to concerns that it may stifle free speech. The crucial question is whether the Act is a justifiable limit of the right to freedom of expression in New Zealand, as provided for in the *New Zealand Bill of Rights Act 1990* (NZBORA), which states that there may be only "such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society".

The HDC Act is intended to cover a wide range of digital communications, including the disclosure of sensitive personal facts and discrimination for colour, race, ethnicity, religion, gender, sexual orientation or disability. It mandates the establishment of an "Approved Agency" (Agency) to advocate on behalf of complainants, which should be helpful by acting as a third party which can mediate and remove unnecessary complaints.

Should the agency decide not to continue investigating a complaint, the complainant has the right to apply to a District Court for an order under the Act. The Agency may opt to not investigate or discontinue investigating complaints which are trivial, unlikely to cause harm, or which do not fall under the Act's "communications principles". The Act clearly intends to cover children and adults as it broadly states that any individual, or their parent, guardian or school leader may apply to the District Court for an order if her or she "has suffered or will suffer harm" from digital communications.

The District Court may issue a wide range of orders including that the material be removed, that the defendant refrain from the conduct in question, that the material be corrected or that an apology be published. In making an order, a court must consider factors such as the communication's content, the level of harm caused or "likely to be caused", its purpose, its audience, the target's age and vulnerability and the public interest.

Terms used – such as "harm" and "offence" – are particularly subjective. "Harm" is defined as "serious emotional distress", which any politician could claim in order to have revelatory content removed. University of Otago Political Studies lecturer Dr Bryce Edwards hypothesised that the Act could legally ban "serious TV journalism", or work such as Nicky Hager's book, if he had published solely online. Thus the Act threatens to criminalise people for exposing politicians, and sensitive subjects such as religion and satire could run afoul of the new law.

The Act provides that online content hosts may opt in to a "safe harbour" provision which shields them from liability provided that they take down "offending" content within 48 hours of receiving a complaint. This section will both protect them from liability but, arguably, impinge freedom of speech. (For more on this, see the article on this topic by Andrew Easterbrook opposite on page 7 of this issue.)

Although the Act specifically requires the Agency and the District Court to act consistently with the "rights and freedoms contained in the *New Zealand Bill of Rights Act 1990*", one of the central concerns is that the Act will impinge free speech in New Zealand. Freedom of speech is covered by section 14 of the NZBORA. The *Human Rights Act 1993* already prohibits hate speech under sections 61 and 131, which have rarely been used.

Critics contend that, while the Act is well-intentioned, it is far too broad and employs subjective definitions. The Act includes "any text message, writing, photography, picture, recording, or other matter that is communicated electronically" under the definition of "digital communication". The penalty is up to two years' imprisonment or a fine of up to $50,000, which is by no means a small penalty.

Terms used – such as "harm" and "offence" – are particularly subjective. "Harm" is defined as "serious emotional distress", which any politician could claim in order to have revelatory content removed. But this law is not limited in scope to people in power. It could theoretically target children who have posted offensive content – for example, to schoolmates. University of Otago Political Studies lecturer Dr Bryce Edwards hypothesised that the Act could legally ban "serious TV journalism", or work such as Nicky Hager's book, if he had published solely online. Thus the Act threatens to criminalise people for exposing politicians, and sensitive subjects such as religion and satire could run afoul of the new law.

In fact, the law may actually facilitate bullying, or at least bullying those with different opinions. Tech blogger Cory Doctorow criticises the Act's "takedown" process, explaining that "trolls who mass-dox or denial-of-service attack a victim could make all of her online presence disappear with impunity and face no penalties at all for abusing the procedure". It is questionable whether sensitive victims would really want to disclose their home address and other details. Moreover, if a poster misses the 48-hour window to respond to the takedown, they lack a legal recourse to justice. Edwards postulates that internet providers may simply remove content rather than go through the complex process of determining a complaint's validity.

Crucially, the law makes some conduct, which would not otherwise be an offence if done offline, an offence if done online. Indeed, apart from making an arbitrary distinction between the online and offline worlds, the law fails to address real-world problems. The authorities could, in preference, make use of and modernise existing laws, such as updating the *Crimes Act 1961*'s provisions against intimate covert filming to include "revenge porn", or by extending the *Harassment Act 1997* to include "digital communications".

The HDC Act is broadly worded and subjective and, as such, poses a threat to online free speech in New Zealand. The Act was proposed with inarguably noble intentions, however, it has the potential to stifle public interest stories and unpopular opinions, especially concerning divisive issues. The Act cannot address offline problems.

Overall, the Act does seem too broad to be a reasonable limit to the right to freedom of speech. Nevertheless, given the non-use of existing legislation in this very area, it remains to be seen whether these fears will be realised. LN

+ *Harmful Digital Communications Act 2015*

Harmful Digital Communications "safe harbour"

By Andrew Easterbrook, Senior Lawyer, Webb Ross McNab Kilpatrick Lawyers, Whangarei

The *Harmful Digital Communications Act 2015* (HDC Act) was enacted on 2 July 2015. Sections 23 to 25 of the HDC Act set out a broad "safe harbour". If certain steps are followed, the safe harbour protects an online host against almost all liability for content hosted on its platform. This article explains the safe harbour and discusses a few things to consider if you are asked to provide advice about it.

A brief explanation of how the safe harbour works is a good starting point. It applies to online content hosts. An online content host is a person who has control over an online system on which content is accessible to users. That includes Facebook, parts of Google, *The New Zealand Herald*, most bloggers, and you (if you have a website on which people can post their own content or comments).

The safe harbour provisions are already in effect, as is the criminal offence of causing harm by posting a digital communication. The remainder of the HDC Act will not come into force until regulations have been drafted. When a user does not like certain content that is available online, that user can complain to the host of that content rather than the author of the content. If the user does that, then provided the host follows certain steps and meets certain criteria set out in section 24, the host cannot be sued. I made a flowchart setting out the process for hosts in some detail, which follows on pages 8 and 9.

The protection afforded to hosts by section 24 does not protect against content posted or procured by the host itself, against copyright liability, breach of a suppression order or breach of bail reporting requirements. But except for those matters, if the host follows section 24, no other content posted by users and hosted by a host can give rise to proceedings against the host. That means:

- Hosts are protected against liability for defamation. That expands the protection already afforded to online hosts by a limited definition of "publisher". The Court of Appeal in *Murray v Wishart* [2014] NZCA 461 held that the person who controls a Facebook page is a publisher of information posted by third parties on that page only if the controller has actual knowledge of the allegedly defamatory post and fails to remove it within a reasonable time. Similar reasoning is likely to apply to the owners of blogs, media sites and other websites that allow comments or self-publishing. But now, even if a host does have actual knowledge of defamatory content, if it follows the process in section 24 then it will be protected against liability. Sometimes that will result in the content being left online. Note that this does not prevent a host from arguing (as per *Murray v Wishart*) that it is not a publisher (section 23(3) preserves that and any other defence that would otherwise be available).

Andrew Easterbrook

- The tort of invasion of privacy will not be available against a host. To my knowledge that has not yet been the subject of proceedings, but the safe harbour will now prevent that from happening. By way of example, if a visitor to the WhaleOil blog were to post pictures of Dan Carter's children, Mr Slater will be protected from liability provided he follows the section 24 process and does not re-publish them.
- Other areas that the safe harbour might restrict liability include: liability under the HDC Act itself (for example, hosting content that incites suicide), the *Human Rights Act 1993* (for example, publishing material that incites racial disharmony), breaches of the *Privacy Act 1993*, breach of confidence, or crimes that involve publishing (for example, the unauthorised disclosure of official information). It would also appear to prevent a host from being classified as a party to any offending under section 66 of the *Crimes Act*.

Issues to consider

First, the safe harbour process must be followed to the letter, or the host loses its protection. If a host receives a notice of complaint and contacts the author, but the author doesn't consent to the takedown, the content must be left in place. It is not hard to imagine situations in which the host would prefer to remove the content once brought to its attention (for example, if it is clearly objectionable), or is pressured by a member of the police or some other agency to remove the content. But if it does remove content without the author's consent, it loses the safe harbour protection.

Second, there is now a gap in copyright liability protection for hosts. Under the *Copyright Act 1994*, section 92C provides a safe harbour for copyright infringement if (upon notice) the content is taken down "as soon as possible" after becoming aware of the content.

If an invalid notice is given to a host under section 24 of the HDC Act, or infringing material is otherwise brought to the host's attention without complaint, then the host will be aware of the content, but does not immediately obtain the protection of the HDC safe harbour. To get that protection the host needs a valid notice of complaint. It also needs to leave the content up, unless it is able to contact the author and the author consents to the takedown, or if it does not receive a response from the author within 48 hours of contacting him or her. So the host might be faced with a difficult choice if the content is both harmful and potentially in breach of copyright. It can take down the content immediately and obtain copyright protection, but lose the wider safe harbour in the HDC Act. Or it can follow the section 24 safe harbour process, but risk losing protection under the *Copyright Act*.

Third, hosts must have an easily accessible mechanism for users to report content under the HDC Act. That is a prerequisite for obtaining protection against liability. But that mechanism may be open to abuse. There is no penalty for making a false complaint or misrepresentation. Content that is not harmful but someone wants to suppress could disappear if a malicious complaint is received but the author cannot be contacted. Anything posted anonymously could well be removed if just one person on the internet doesn't like it.

On the other end of the spectrum, a controversial piece of content that goes viral could be the subject of hundreds (or thousands) of complaints. A host could easily be overwhelmed if it attempts to address each complaint. However, to get safe harbour protection, a host arguably only needs to respond in full to the first complaint made about specific content. If the section 24 process is followed in relation to one complaint about specific content, then the safe harbour provides protection against any proceedings by any person in relation to that same content. It does not appear that section 24 protection is lost if a subsequent complaint in respect of specific content is ignored.

But protection could be lost if hosts respond incorrectly to a later complaint. For example, if an author does not respond to a later complaint (because he or she doesn't have to) and the host removes the content, then the removal would breach section 24(2)(d) and the host would lose the protection it obtained by correctly processing the first complaint.

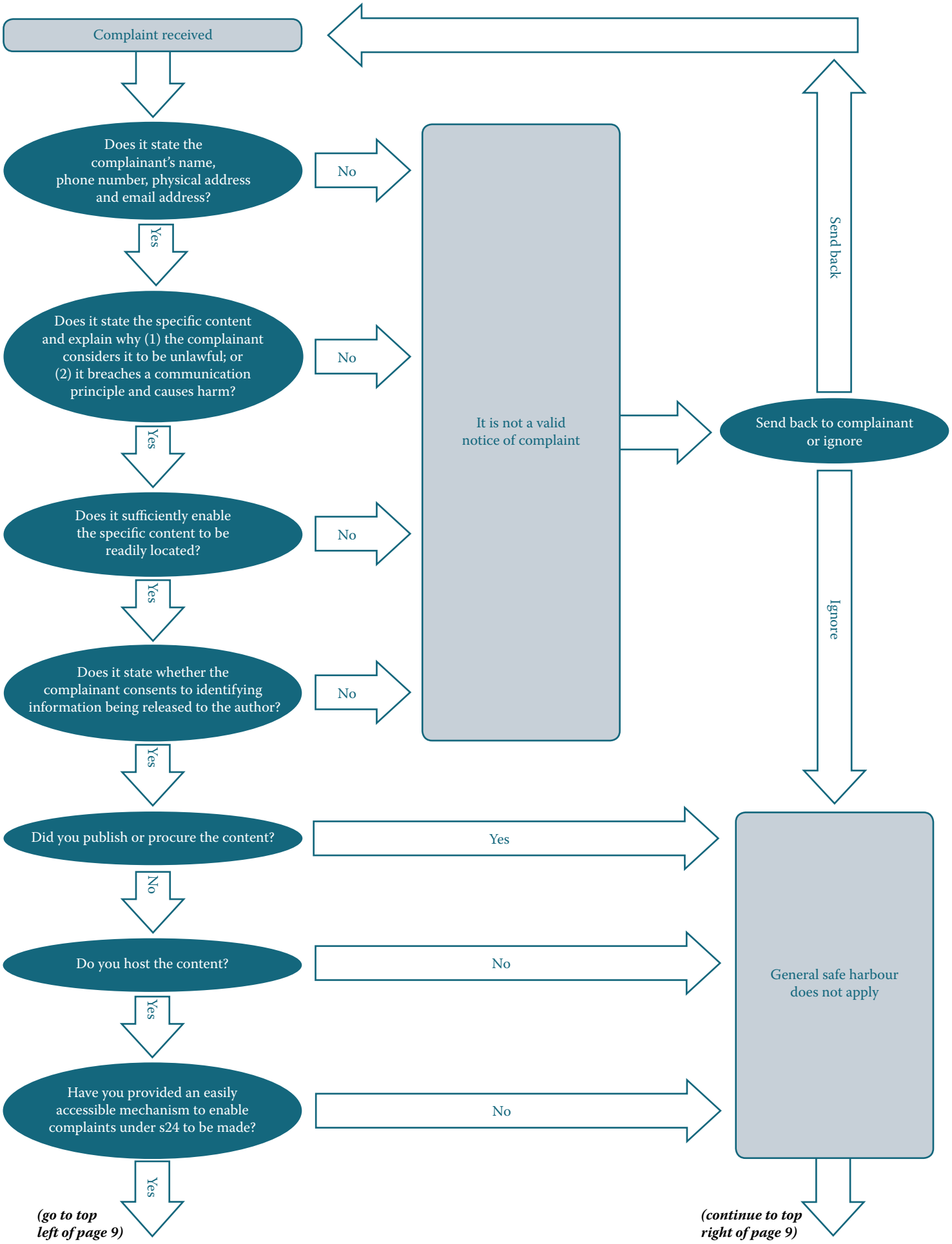
Hosts should therefore maintain a register of complaints. Ideally, whatever reporting mechanism is put in place would check the URL of the offending content against a database of previous reports, and add a flag to the notice of compliant if it has already been dealt with.

It will be interesting to see how the courts respond to hosts seeking safe harbour protection over the next few years. It will also be interesting to see if the complaint system is abused, and if so whether certain large internet companies will – despite the increased risk of liability – refuse to remove content that is the subject of malicious or vexatious complaints.

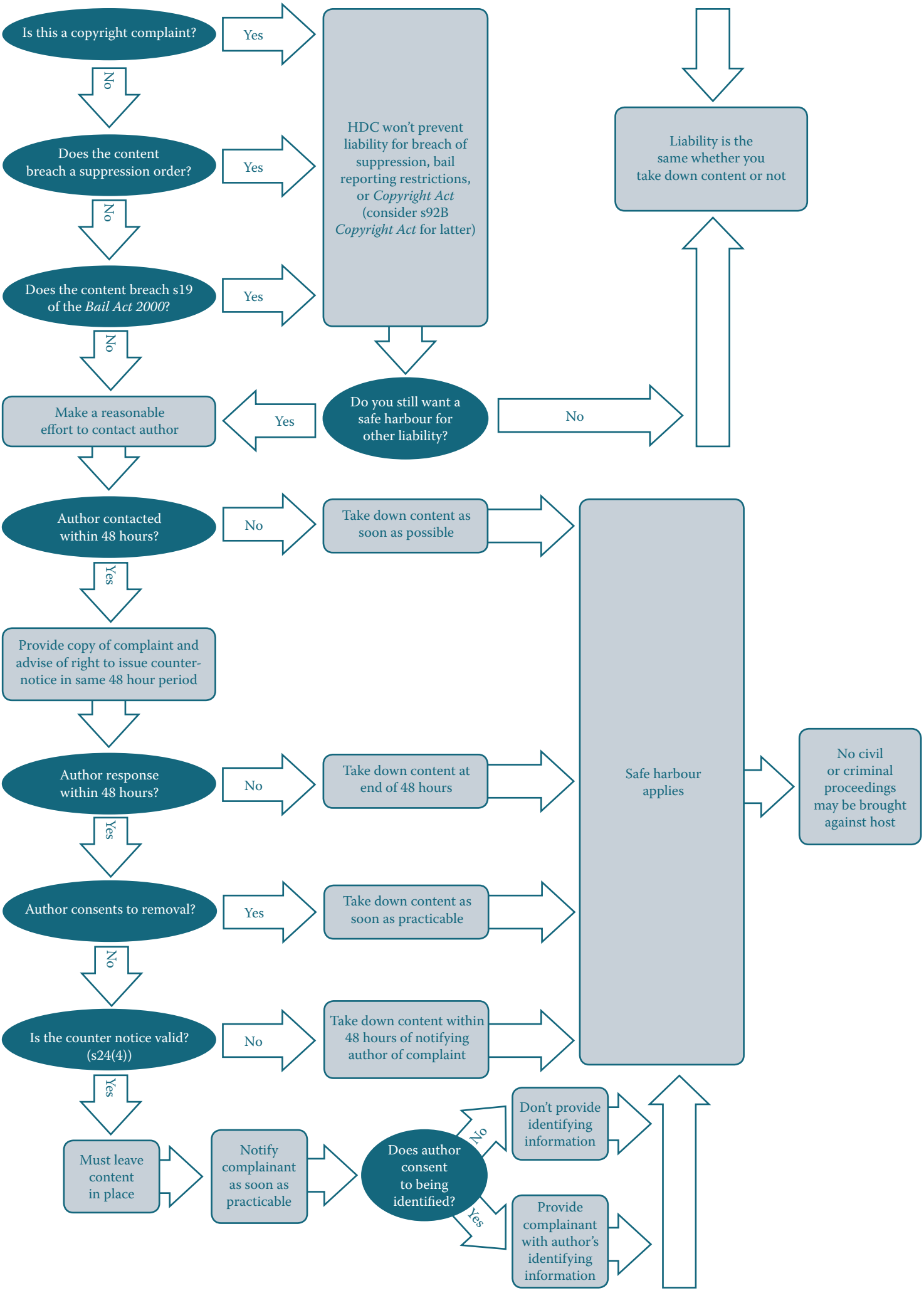
Continued on page 8

Continued from page 7, "Harmful Digital Communications "safe harbour"

Harmful Digital Communications Act 2015 – are you protected from liability?



Continued from page 8



Some useful IT terms and tips for lawyers

By Arran Hunt, Solicitor, Turner Hopkins

Technology is finding its way into many of the matters we deal with.

Whilst most lawyers will only have a rudimentary understanding of the technology, we should all be familiar with at least some of the basic terms.

What is provided here are just some of the terms you may come across, and the explanations are meant to provide a basic understanding only.

Bit v byte – These are a measure of data size, both in data transfer and data storage. A byte (shown as a large B as in 100 MB) is made up of 8 bits (shown as a small b as in 100 Mb). Bytes are usually used as a way to show storage size, bits are usually used to show speed.

Deepweb & Darknet – Google and other search engines provide an index of only a portion of the Internet. There are large parts of the World Wide Web that Google does not index, and this is called the Deepweb. Below that is the Darknet, a portion of the Internet that is only accessible through special technology (such as connections directly between known computers) or through software like Tor. The use of such software on the Darknet makes it extremely difficult for authorities to monitor activities, making it the ideal place for the trade in illicit materials and terrorist communications.


Arran Hunt

Distributed Denial of Service Attack – A DDoS is an attack on an internet connection conducted through brute force. Using many separate computers (possibly numbering in the tens of thousands), the attacker has all of the machines attempt communication with the target at once. In the same way a person would have difficulty talking to thousands of people at once, the target is often overwhelmed and its internet connection becomes unusable. Such attacks could last days or weeks, and are often performed using computers which have been infected with software without the owners knowing, making it difficult to trace the source of the attack.

Domain name – The internet works on numbers (see IPV4). To make things more user-friendly, people can buy a domain name. A domain name service (abbreviated DNS and run by large companies such as Google) then translates the domain name someone enters (such as www.google.co.nz) into its numerical equivalent, which the computers use to communicate.

Internet – The internet is the network that connects the computers around the world. It is more than just the World Wide Web and features a number of other technologies such as VOIP and the Darkweb.

Internet of Things (IOT) – This is the idea that all objects in the world communicate with each other without human interaction. It is becoming a reality as more devices include access with the internet, usually by WiFi. An example of this technology already in use includes your phone

Continued on page 11

10 tips for drafting IT into contracts

IT has embedded itself into society and many of our clients will now require elements of IT in many of the documents they need. Here are some tips to hopefully assist you in drafting those IT clauses:

1. ***"The Internet" and "the Web" are two different things*** – The World Wide Web forms just a part of the Internet, being webpages accessed through a browser. Don't refer to the Web unless you intend to restrict your meaning to just the Web, as you will be missing many other technologies such as Skype or WhatsApp. It is better to use the word Internet.
2. ***Don't list websites or internet services unless you need to be specific*** – Listing a particular website, such as Facebook, when the contract is looking to cover the Internet as a whole, provides no benefit and could create confusion as to whether you are limiting the effect of the document.
3. ***Unless you are dealing in an intangible asset …*** – If you are dealing with an intangible asset, such as a domain name or a social media account, then be as specific as possible. List the location and what is being dealt with (for example, is it just the right to use that login name, or the current user account and all it contains?).
4. ***Don't list technologies unless needed*** – Technology develops quickly, and specifying different technologies may mean missing out on things in the future. For example, listing a particular version of an operating system, or the use of ADSL, would rule out future upgrades to the operating system or faster internet connections, effectively requiring the contracted party to retain obsolete technology.
5. ***Give your staff some credit …*** – Dependent on the role, internet access can be a boon for staff, providing an almost limitless font of knowledge. Overly restrictive company policies, to control internet use, could actually stifle staff ability to perform their jobs by accidentally blocking staff from accessing websites or services that can help them perform their jobs.
6. ***… however, not too much*** – It is also important that staff members are aware of the limitations of their access, and that it should be used for work purposes. Employment agreements can outline any company policies regarding the use of the internet, such as the use of company IP on the staff members' social media pages.
7. ***Intellectual property*** – Intellectual property now makes up the majority of value in most large companies. Make sure that your clients' IP needs are just as protected as their physical assets.
8. ***Know what you're drafting*** – While you won't need a complete working knowledge of your clients' products, you need to have a reasonable understanding so that you can adequately protect them. I follow Einstein's approach to knowing something; if I can't explain it simply, I don't know it well enough. It is better for you to ask questions of your client than for your documents to be found lacking.
9. ***If you don't know it well enough …*** – If you don't know your client's business well enough, and you can't learn it well enough to provide them the service they need, then it is better to pass the matter to a specialist.
10. ***Trust nobody online*** – Many prestigious companies have been caught by people calling and pretending to provide IT advice or to alert them to an issue. If you receive such a call refer them to your IT service provider.

… and an extra one for free…

11. ***IT is actually quite simple*** – People have a fear of the unknown, and for many IT is the ultimate unknown. If you have someone who can explain things simply, people will often be able to grasp what something does, if not how it works.

Continued from page 10

notifying your home heating to switch on as you travel your typical path home. Use of IOT is expected to grow rapidly in the coming years.

IPV4 – When the Internet was created, an address system was created using four digits each ranging from 0 to 255. When a computer accesses the Internet it is allocated one of these codes, called an IP address, such as 168.201.23.197. This creates a limited number of addresses available, much fewer than is needed. Luckily multiple users can share an IP address. However, even with IP sharing, the growth of the Internet (with IOT) means that the number of IP addresses available is insufficient.

IPV6 – As IPV4 doesn't provide enough addresses, a new form of address was created called IPV6. Without explaining how it works, it provides substantially more distinct IP addresses. Whereas IPV4 has 4.3 billion distinct addresses, IPV6 allows for 340 undecillion (that is 34 followed by 37 zeroes) – enough for approximately 10 addresses per square inch of the planet.

Tor – Tor is software that helps to anonymise internet users by passing information through other Tor users randomly, making it difficult to tell who the end user is. Software of this type is widely used to access internet services that may be otherwise blocked by internet service providers or governments (such as China's block on various websites).

VOIP – Voice Over Internet Protocol is the technology used to make phone calls over the internet rather than over traditional phone lines. It is not restricted to just computer-based calls, with many office networks now using VOIP phones and include phone numbers, faxes etc.

World Wide Web – Created by Sir Tim Berners-Lee, it is the collection of pages linked together with hyperlinks (where you click on an underlined word or image and it takes you to another page). The Web is the most commonly used part of the Internet and it is what you are accessing when you use Internet Explorer or Chrome to access a webpage. LN

10 tips for obtaining the right IT services for your firm

1. ***Look at your legal obligations*** – It is important that you understand what your requirements are. This includes your requirements to client confidentiality, notice requirements under the *Companies Act 1993*, *Electronic Transactions Act 2012* and others. A good IT service provider should know some of these, especially if they have other legal clients, however those liabilities fall on you.
2. ***Don't overstep your knowledge*** – Go into the procedure with a few basic requirements, but allow the IT service providers to suggest new technologies and procedures that you may not have considered.
3. ***Everything is at a price*** – Once you know what is available, look at the cost versus the benefit. Almost everything is possible, but it is all at a cost.
4. ***Lawyers don't like change*** – Be honest with yourself about what changes you will make. There is no point spending money on something if you will not change your procedures and use it.
5. ***Cost is not the only factor*** – While the cost is important, look at the time you spend doing repetitive tasks that could be replaced. A small cost could equal several more billable units per day per author.
6. ***Use your internal expertise*** – If you have a solicitor who has IT knowledge, make use of it by allowing them to be part of the process.
7. ***Bigger is not always better*** – Look for IT service providers who best fit your structure. A larger firm will need to look for larger service providers who have enough staff to provide adequate cover. However, smaller boutique firms may find smaller IT service providers (even sole traders) can provide a more tailored and personal experience, and often at a better cost.
8. ***Storage is cheap*** – Electronic storage is cheap, as is the cost of internet bandwidth. Talk to your IT service provider about removing limits on email size, so that you don't miss important emails because the attached document is too large. Clients shouldn't need to be asked to break up a document because your system prevents a large document being received.
9. ***Security is important*** – Lawyers often deal with their clients' most private and confidential matters, so it is important that these are secured correctly. All PCs should have passwords, backups should be encrypted and remote access should have several levels of security.
10. ***Use the Cloud but with caution and only when needed*** – The Cloud can be a huge advantage, but its usefulness is largely dependent on how it is utilised. All firms should look at having their data backed up over the Cloud (as well as locally) as this removes the risk from localised disasters (such as the Christchurch earthquakes) and allows you to retrieve the data from another location. Make sure that your Cloud backups are being stored in New Zealand so as to limit any jurisdictional issues. Other Cloud functions, such as the ability to work anywhere with virtual servers and virtual desktops, can be useful to certain users but can be expensive, so be honest with whether you will use these features (and any downsides that such technologies can create).

Introduction to "Cloud computing"

By Lloyd Gallagher, Director/Arbitrator/ Mediator, Gallagher & Co Consultants Ltd

Cloud computing is fast changing the way we handle information. The cost savings and ease of access makes Cloud computing not only a tempting technology, but one companies often rush into without looking at the full range of issues associated with offsite data storage.

These issues are relevant both in terms of the internal workings of a law firm, as well as for clients seeking legal advice in relation to their own uptake of Cloud services. In addition, a number of Cloud suppliers have rushed to provide offerings to satisfy what they see as a necessity for customer demand without adequately developing contracts that satisfy industry needs.

This has led to a number of problems that has resulted in costly legal action and loss of data or lock-in (an industry term used when a user wishes to move their data to another provider but is unable to do so due to an incompatibility in the standard used to supply the Cloud service or limited termination clauses). Further, the inflexibility of contracts provided by many Cloud service providers leaves law firms at risk of breaching their professional responsibilities.

This article is the first in a series which will traverse the technical issues and demystify some of the jargon of Cloud computing, while highlighting the legal responsibilities that law firms need to be aware of when becoming clients of Cloud services. This, in turn, should help firms develop a better guideline for providing legal advice around these services. Future articles will appear in upcoming issues of *Law News* through the year.

What is Cloud computing?

A number of issues are present in Cloud computing that can cause law firms distinct problems when adopting the services. However, before we get to those issues, it is important to understand some basics of Cloud computing services as a whole. The term "Cloud computing" is currently used as a marketing term but there is no agreed definition as such in relation to how companies advertise their services and what is truly considered a Cloud service as compared to just off-site storage ("Cloud Computing: The Concept, Impacts and the Role of Government Policy", *OECD Digital Economy Papers*, No. 240).

This marketing term, while not incorrect, has caused considerable debate and confusion that led to a formal draft definition from the US National Institute of Standards and Technology (NIST) and Berkeley RAD Lab that could be used in legislation (Mell, P. & Grance, T. (US National Institute of Standards and Technology) "The NIST Definition of Cloud Computing" (2011) <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>; Armbrust, N. et al. "Above the Cloud: A Berkeley View of Cloud Computing" (2009) http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf).


Lloyd Gallagher

The OECD suggests that where these two bodies concur, a clear understanding is created and the following definition can be created:

"Cloud computing can be understood as a service model for computing services based on a set of computing resources that can be accessed in a flexible elastic, on-demand way with low management effort."

The result is that any of the following services can be deemed a Cloud service:

- ***SaaS (Software as a Service):***

  In the SaaS model, Cloud users directly access the applications of the Cloud provider and therefore have the convenience of not having to manage the underlying infrastructure or the capabilities of the applications. SaaS Cloud services include applications for specific business processes and purposes. The spectrum of examples is large and ranges from e-mail applications used by consumers to business applications and integrated management software solutions such as customer relationship management (CRM) tools, document management or accounting solutions, to name just a few.

- ***PaaS (Platform as a Service):***

  Platform as a Service (PaaS) provides users a more structured platform to deploy their own applications and services. Typically, users rely on programming languages and further tools of the Cloud provider to deploy these applications. Cloud users do not manage or control the underlying infrastructure such as networks or operating systems, with the service provider managing the virtualisation operations. Suppliers of PaaS use dedicated application programming interfaces (APIs). As each Cloud provider generally relies on its own API, it is typically difficult to move applications from one Cloud provider to the other. There are initial attempts, however, to develop generic programming models. Examples for PaaS include the Windows Azure Platform and the Google App Engine.

- ***IaaS (Infrastructure as a Service):***

  Infrastructure as a Service (IaaS) provides computing resources such as processing, storage and networks to the users of Clouds, and enables users to leverage these resources through their own implementation of virtualisation capabilities. Providers of these hardware virtual machines offer access to raw computing resources and a high degree of flexibility. IaaS users are able to access computational resources (e.g. CPUs), and run operating systems and software on the provided computing resources. The flexibility for users is very high in the IaaS model as there are only a few limits on the kinds of application that can be hosted on these services. Examples of services that fall into the IaaS category include Amazon Elastic Cloud (EC) 2 and Zimory.

This definition then reduces further to a number of deployment models which are defined as follows:

- ***Public Cloud:***

  Services are generally owned by the service provider and resources are shared between the company and the general public.

- ***Private Cloud:***

  Services are owned or leased by a single company and the underlying hardware and software is not shared with anyone else. These can be located onsite or offsite.

- ***Community Clouds:***

  These can be both public and/or private and are generally shared amongst a group with common concerns. In the community Cloud resources can be shared amongst the common group, for example, a law firm sharing services with all staff or a group of firms sharing a common goal. Microsoft's sharepoint server is an example of a community designed Cloud.

- ***Hybrid Clouds:***

  As the name suggests, a hybrid Cloud can be a combination or mix of the above definitions. In a hybrid Cloud a secure service can be deployed in a private Cloud infrastructure that also combines community access for staff in the same firm. This also provides a level of flexibility for on demand increase in resources and the scaling back of resources when they are no longer needed.

Some examples of Cloud computing are Amazon's EC2, RackSpace Cloud, and Google's Cloud Platform. These deployment models and services provide an endless range of solutions for the Cloud user, from improved backup/disaster recovery and flexibility of scale with on demand

Continued on page 13

Continued from page 12

resource increase, to reduced IT support and less frequent updates to software. However, these benefits also come with a range of pitfalls, as discussed below.

Cloud computing – issues and benefits

Cloud computing has a range of potential deployments that can provide substantial benefits to users (including law firms) in cost reductions as well as on demand scalability. However, these services are not without their pitfalls and adopters need to carefully consider the implications of adoption before committing to Cloud services for their firm. Below, I will outline a general introduction to each benefit and pitfall in turn, however, due to the limited size of this article detailed explanation of each will be dealt with in future articles in this series.

Taxes

One of the most immediate benefits of Cloud services is in taxes. The implementation of Cloud infrastructure allows the firm to transfer its IT budget from capital expenditure to operating expenditure. This sees an immediate improvement for income tax, as assets are no longer pooled into capital depreciation but are given the normal operating expenditure treatment under the *Income Tax Act 2007*.

However, where the service is provided by an overseas provider, it is important to note that GST is zero-rated due to the non-resident nature of the service provider (see the IRD's discussion on "e-Commerce and GST", available from the IRD's website www.ird.govt.nz/ecommerce-tax).

Further, a number of legal issues arise with reporting obligations under the Revenue Acts which pose particular issues for tax agents, accountants, law firms and tax payers directly. This will be dealt with in depth in a future article that will also discuss implications for general electronic retention, but for now, practitioners must be mindful to investigate the issues before simply adopting Cloud services, otherwise they may face issues of non-compliance from the Commissioner.

Elasticity

Another immediate improvement is the cost savings in IT manpower. Cloud services provide managed infrastructure and automatic software updates that reduce the need for IT staff. Further, resources can be applied on demand and as needed resulting in less IT callouts for server provisioning and maintenance.

However, drawbacks exist in the loss of IT control and the security risks of storing client data offsite. The loss of IT control can occur from a range of sources such as service outage, internet congestion, and reliance on the service provider's control over applications.

When deciding on service provision, law firms should consider carefully how the service is provided, what redundancies are in place, what happens if a physical connection (fibre, ADSL etc) fails, and can the service provider force an upgrade to a version that may not be right or compatible for the firm's current use, or shut down an application that the firm relies upon? These are very real issues that must be considered and could result in lock-in occurring for access (which I will deal with in depth in a later article in this series).

Privacy

Holding client data offshore has both benefits and pitfalls in the protection and retention of both client and the firm's data. New Zealand law imposes a range of specific duties on both the privacy of client data as well as professional duties on law firms retaining that data, even if that data is held in offshore data centres.

The current Cloud computing models and contracts pose particular problems for law firms that could easily result in the firm facing issues of non-compliance under the Lawyers and Conveyancers Act (Lawyers: Conduct and Client Care) Rules 2008. This is a large area that will be discussed in a future article, but the issue is of such high importance that I consider it necessary to comment here before firms rush into Cloud implementation.

Security

Privacy issues are also present in the way Cloud services provide security. Poor security implementation, and poor contract controls, can result in data being obtained by third parties in a number of ways.

One such way is the sale of client contact details by Cloud service providers. Another is intrusion and download of entire systems. Further, Cloud supply companies can be at fault where the service is operated by inexperienced providers who simply resell data centre infrastructure.

A number of topologies exist for security provisioning but not all providers have implemented such measures and firms may be found negligent if they have not properly investigated the service provides implementation of security. This, and details of what to look for, will be dealt with in a future article.

Outages, access and lock-ins

Once the above concerns have been resolved, the next issue to look at is what happens when things go wrong. This can be termed as outages (physical internet communication failure), access (what happens when the Cloud service is offline and you have to file in court), and lock-ins (what if we want to move service – are the applications we use compatible with the new provider?).

While outages and access can be mitigated through backup systems and choosing providers with redundancy setups, the issue of lock-ins pose particular difficulties due to the lack of Cloud computing standards. There have been some horror stories of companies finding themselves locked into contracts with a cloud supplier due to a lack of standardisation or contract termination provisions.

These questions will be dealt with in depth in a future article but firms need to be conscious of ever-changing Cloud standards that can affect usability and ease of transfer to new providers if contract negotiations break down.

Should we even move?

Finally, firms have been seen to jump on the promise of Cloud computing before they have fully checked to see if it is the right thing for their firm. A number of solutions exist for both in-house and external provisioning and firms should investigate properly what solution best fits their staff needs, their duties of compliance, and whether the Cloud will actually generate better performance.

In a future article, I will look into all the options available and discuss the questions you need to look at when deciding if a move to the Cloud is right for your firm.

Conclusion

Cloud computing provides substantial cost savings, tax benefits and ease of access from a range of devices. However, it comes with a heavy burden in security, privacy protection and reporting obligations under law. Further, many firms move to the Cloud before they consciously consider if a move actually works for them.

Over the coming publications I will discuss these issues at length with an aim to help you understand what to look for when advising your clients and/or choosing a Cloud service for your firm. LN

Selected CPD

To view all ADLSI CPD & register: www.adls.org.nz/cpd

Email us: cpd@adls.org.nz | Phone us: 09 303 5278

ADLSI CPD
Experts in accessible relevant legal learning

Featured CPD

Tuesday
1 September 2015
12pm – 1pm

1 CPD HOUR

Webinar

A 'Capital Idea' – Getting to Grips with the New Residential Land Tax Rules

Taxing the gains from property speculation as a mechanism to cool down the overheated Auckland property market is a significant Government initiative with proposed new "bright-line" tax rules designed to take effect from 1 October 2015.

Learning Outcomes

Become familiar with:

- the new bright-line tax rules and what land transactions they apply to;
- any exemptions from the rules and how the rules interact with existing tax rules applying to land transactions;
- the nature of advice and warnings that will need to be given to clients in terms of reporting and other related obligations; and
- the rules that will capture transactions made through related-ownership vehicles.

Who should attend?

Property lawyers and legal executives, trust lawyers, commercial lawyers and general practitioners advising clients on property investment strategies.

Presenter: **Denham Martin**, Barrister

Thursday
24 September
2015
4pm – 6.15pm

2 CPD HOURS

Seminar Live stream

Property Law Pot Pourri 2015

The Sale and Purchase of Managed Units

This presentation will provide advice on how best to represent both sellers and purchasers when entering into transactions involving managed units, with focus on the variety of management agreements that exist.

Easements and Covenants

This session will consider the nature, uses and interpretation of easements and covenants, as well as current issues.

Authority and Instruction Forms

Our presenter from LINZ will consider problems that may arise with A&I Forms and possible solutions.

Who should attend?

All lawyers and legal executives practising in the area of property law.

Presenters: **Denise Marsden**, Partner, Alexander Dorrington; **Thomas Gibbons**, Director, McCaw Lewis Lawyers (Hamilton); **David Chapman**, Senior Advisor, LINZ

Thursday
3 September 2015
4pm – 6.15pm

2 CPD HOURS

Seminar Live stream

The Devil You Know: Gathering & Providing Information in Relationship Property Cases

Knowing the nature, value and status of assets and liabilities is fundamental to the division of relationship property. Obtaining that information is therefore essential. This seminar canvases the different ways to extract information and the implications of those choices.

Learning outcomes

- Gain a better understanding of the various methods for gathering information.
- Gain a greater awareness of the obligations around discovery and disclosure, including in relation to s 21 agreements.
- Become more familiar with the various court and professional rules which apply to gathering and providing relationship property information.

Who should attend?

All lawyers who act in relationship property cases and advise on relationship property settlements and agreements.

Presenters: **Jane Hunter**, Barrister, Southern Cross Chambers; **Mark Vickerman**, Barrister, O'Connell Chambers

Chair: **His Honour Principal Family Court Judge L Ryan** *Facilitator:* **Stuart Cummings**, Barrister, Surrey Chambers

---

Wednesday
16 September
12pm – 1pm

1 CPD HOUR

Webinar

Rural Law Series: The Ins and Outs of Rural Syndications

Syndication has obvious advantages for farmers and investors alike but the process is complex and needs to be handled with care from start to finish. This webinar will discuss reasons for syndication and how the syndication process is managed.

Learning Outcomes

- Gain insights into farm syndication trends, who is entering into syndications, the reasons why and in which sectors the process is occurring.
- Obtain an overview of the syndication process.
- Learn more about the numerous factors that need to be investigated before syndication is entered into.
- Understand better the syndication models of Closely Held and Professionally Promoted Entities and the implications of the Financial Markets Conduct Act on the latter.
- Gain a more comprehensive understanding of the key agreement and other transaction documents.

Who should attend?

Rural lawyers, and property and commercial practitioners advising clients on the syndication process.

Presenter: **Brett Gould**, Partner, Gibson Sheat

CPD in Brief

Independent Trustees: Avoiding the Perils of Personal Liability

Wednesday 19 August 2015 | 12pm – 1pm

The role of the independent trustee appears to be increasingly onerous. The consequences of even minor oversights are often severe and can cost a trustee dearly, both financially and professionally. Understanding the duties and obligations associated with being a trustee, and how best to ensure compliance with those duties and obligations, is crucial for lawyers both acting as trustees and advising clients taking on the role of trustee.

Presenter: **Tammy McLeod**, Director, Davenports Harbour Lawyers

Webinar

Funds Transfer Pricing and Debt Capitalisation & Remission

Wednesday 26 August 2015 | 12pm – 1pm

Over 50% of our foreign-owned companies are owned by our major trading partners, including Australia. In an environment where particular government attention is being directed at base erosion profit shifting, it is more important than ever to price related-party funding correctly.

Presenter: **Paul Hale**, Principal Advisor – Financial Arrangements, Inland Revenue

Webinar

Immigration Law: Making Good Use of Useful International Conventions

Wednesday 2 September 2015 | 12pm – 1pm

International obligations, such as the UN Convention on the Rights of the Child, inform many decisions made under the Immigration Act. This webinar introduces the most useful conventions and shows you when and how to use them effectively.

Presenter: **Martin Treadwell**, Deputy Chair, Immigration and Protection Tribunal

Webinar

Preserving Assets: A Litigator's Armoury for Interim Relief

Thursday 10 September 2015 | 4pm – 6.15pm

Preserving assets may mean the difference between a Pyrrhic victory and one for which the client will thank you. Litigators have several weapons to achieve this objective: an array of orders (e.g. search, freezing, pre-trial charging), in addition to the Court's jurisdiction to appoint receivers.

Presenters: **Seb Bisley**, Partner, Buddle Findlay; **James Nolen**, Partner, Lowndes

Live stream Seminar

CPD On Demand

Self-Represented Persons: Problems and Solutions – Family Law – 1 CPD HOUR

In the Family law context, where lawyers have been removed from the early stages of some proceedings, emotions run high and funds for legal fees are often restricted, accommodating and managing self-represented persons is becoming increasingly important.

Presenters: **His Honour Judge Maude**; **Lynda Kearns**, Barrister, Bastion Chambers

On Demand

Briefing Psychologists & Understanding their Reports – 1 CPD HOUR

The evidence of mental health experts can be vital to obtaining a successful outcome for a client, whether in the mental health, family or criminal contexts for example. This webinar will enable you to work more effectively with psychologists.

Presenters: **Kate Leys**, Barrister; **Dr John Nuth**, Registered Clinical Psychologist/Neuropsychologist

On Demand

Where There's No Will There's A Way: Intestacy Refresher – 1 CPD HOUR

Not everyone makes a will. This recorded webinar will update you on what to do if one of your clients dies intestate or partially intestate.

Presenters: **Greg Muller**, Director, GM Legal; **Tamara Barker**, Senior Relationship Adviser, Public Trust

On Demand

CPD Pricing

Delivery Method	Member Pricing	Non-Member Pricing
Webinar	$75.00 + GST (= $86.25 incl. GST)	$95.00 + GST (= $109.25 incl. GST)
Seminar (in person)	$125.00 + GST (= $143.75 incl. GST)	$180.00 + GST (= $207.00 incl. GST)
Seminar (live stream)	$125.00 + GST (= $143.75 incl. GST)	$180.00 + GST (= $207.00 incl. GST)
On Demand (1-hour recording)	$85.00 + GST (= $97.75 incl. GST)	$110.00 + GST (= $126.50 incl. GST)
On Demand (2-hour recording)	$95.00 + GST (= $109.25 incl. GST)	$130.00 + GST (= $149.50 incl. GST)

For group bookings for webinars & CPD On Demand, see the ADLSI website at: www.adls.org.nz/cpd/help-and-faqs/group-bookings/.

+ Media law book

Burrows and Cheer Media Law in New Zealand, 7th Edition

Author: Ursula Cheer

Published: July 2015

In this 7th edition, the author has comprehensively updated the text to reflect rapid changes in law since 2010, particularly with regards to defamation, privacy, breach of confidence, contempt and court reporting, official information, and media complaints bodies.

A new chapter on the New Zealand advertising standards regime has also been added. All chapters include well-developed sections on how publication on the internet and other new media is affecting the law.

Price: $152.17 plus GST ($175.00 incl. GST)*

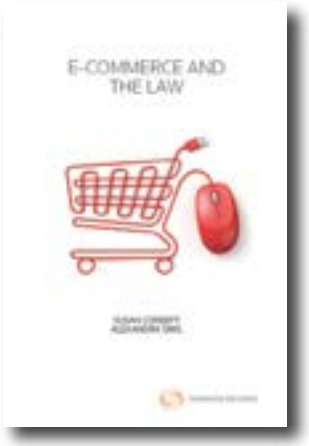
Price for ADLSI Members: $136.95 plus GST ($157.49 incl. GST)*

(+ Postage and packaging)*

To purchase this book, please visit www.adls.org.nz/adlsi-store or contact the ADLSI bookstore by phone: 09 306 5740, fax: 09 306 5741 or email: thestore@adls.org.nz.

+ E-commerce book

E-Commerce and the Law



Authors: Susan Corbett, Alexandra Sims

Published: November 2014

E-Commerce and the Law is an invaluable and user-friendly guide to the legal concepts underpinning, and the law regulating, online business.

Concise, well-researched and up-to-date, this book informs readers about how online businesses can conduct themselves appropriately and what steps can be taken to better protect trademarks, technical systems and sales operations.

Price: $73.91 plus GST ($85.00 incl. GST)*

Price for ADLSI Members: $66.52 plus GST ($76.50 incl. GST)*

(+ Postage and packaging)*

To purchase this book, please visit www.adls.org.nz/adlsi-store or contact the ADLSI bookstore by phone: 09 306 5740, fax: 09 306 5741 or email: thestore@adls.org.nz.

+ ADLSI Committees

Committee membership applications for 2015/16

ADLSI has a proud history of contributing to the law through its active member Committees programme.

Fourteen ADLSI Committees operate at present, comprised of volunteers who carry out a wide range of activities in their specialist areas.

Earlier this year, the ADLSI Council took the decision to align Committee appointments with the financial year. This was done to make the application process easier for our members (previously it took place over the busy Christmas/New Year period) and to enable greater continuity of Committee work.

Applications for places on Committees for the 2015/16 financial year will be open from Monday 17 August 2015. ADLSI encourages applications from members throughout New Zealand, and attendance at meetings includes remote participation via phone and Skype conferencing.

Successful Committee applicants appointed by the ADLSI Council will be notified in late September this year, with the first Committee meetings taking place in October.

New Committee members (and existing Committee members wishing to remain on Committees) should apply online at www.adls.org.nz/for-the-profession/application-for-membership-to-adlsi-committees/ by 5pm, Tuesday 8 September 2015.

For further information or assistance, please contact Helen Young on 09 306 5744 or by email at helen.young@adlsi.org.nz.

Helen Young, Vivian Zhang, Gardenia Atimalala and Denise Wallwork at the 2014 Committees "Thank you" evening

ADLSI has Committees in the following key areas – which might be the one for you?

- Civil Litigation
- Commercial Law
- Continuing Professional Development
- Courthouse Liaison
- Criminal Law
- Documents & Precedents
- Employment Law
- Environment & Resource Management Law
- Family Law
- Immigration & Refugee Law
- Mental Health & Disability Law
- Property Disputes
- Property Law
- Technology & Law

Continued from page 2, "Careful what you wish for – social media in the wake of *Hammond v Credit Union Baywide*"

Ms Hammond should have expected that her information was no longer private when posted to Facebook, but she did not. Agencies should take some responsibility to ensure that their customers or employees are not encouraged to share more personal information online than they are comfortable with.

If an agency wishes to control its employees' use of social media, do it right

Every agency should have a social media policy. If an agency has concerns about the way its employees use social media, then they should make these concerns clear to the employees from the outset. Preventing employee misconduct online by establishing boundaries early on is a safer way to ensure appropriate online behaviour than embarking on elaborate forms of information vigilantism after the fact.

Ensure that all employees understand their *Privacy Act* obligations

A social media policy is only one part of the framework required to ensure that an agency does not fall foul of the *Privacy Act* as a result of thoughtless collections, uses or disclosures of personal information obtained from social networking sites. Ensuring that employees are aware of their obligations under the *Privacy Act*, with clear policies, procedures and training can assist an agency to invoke a legitimate defence when something goes wrong. (See section 126(4) of the *Privacy Act*, which states that an employer is liable for the actions of its employees unless it can establish that it took reasonable steps to prevent the employee from doing those acts.)

Consider what impact, if any, the newly enacted *Harmful Digital Communications Act 2015* could have on the use of social media

While aimed primarily at the actions of individuals and targeting the abhorrent behaviour and appalling consequences of cyber-bullying, this new legislation could have a real impact on the use of publicly available information by agencies. The Act amends principles 10 and 11 of the *Privacy Act*, prohibiting the use or disclosure of publicly available information where in the circumstances such a use or disclosure would be unfair or unreasonable. This limitation on the scope of the publicly available publication exception will require caution on the part of agencies seeking to use or on-disclose any personal information obtained online.

Settlement should be a real consideration in cases such as this

While this article does not suggest that any and all complaints should be settled, regardless of their merit, Baywide appears to have failed to take various opportunities to come to the table and resolve Ms Hammond's concerns. Had Baywide sought appropriate legal advice from the outset, it could have avoided a very public hearing of its actions.

Comments and opinions expressed in this article are those of the author, and do not necessarily represent the views of Sovereign. LN

+ Event, young lawyers

2015 Meredith Connell Greg Everard moot

Participants in this year's Meredith Connell Greg Everard Mooting Competition will debate issues around a poorly constructed development in a refined Auckland suburb.

There are 19 students in the preliminary rounds of the competition, vying to be one of the four finalists who will tackle the topic before the Hon Justice Hinton in the historic No 1 courtroom at the Auckland High Court.

Moot organiser, Senior Lecturer Nina Khouri, says more students than ever before have put their names forward for this year's competition, which starts at 6pm with refreshments and ends with an awards ceremony at 8pm on Wednesday 19 August 2015.

The annual moot is in memory of Greg Everard, an alumnus of the Auckland Law School and a leading civil litigation lawyer who excelled in the discipline of mooting.

It is expected that Mr Everard's colleagues, friends and family, law professionals and keen mooters from the Law School will come along to support the finalists as they debate this year's moot problem concerning the development of an historic, industrial building in a gentrifying suburb of Auckland.

The scenario is that the owner, a charitable trust, engaged a construction company to renovate the building. The finished units were sold to investors, who have leased them to businesses such as hairdressers specialising in moustache and beard upkeep, burger bars, and a Scandinavian furniture store.

Business boomed until water ingress and other structural issues with the building appeared. The construction company has gone into liquidation, its director has fled to Cuba, and the charitable trust and local council now face claims by the investor-purchasers. Having lost in the Moot High Court, the purchasers now appeal to the Moot Court of Appeal.

Date: Wednesday 19 August 2015

Timing: 6:00pm (refreshments and networking); 6:30pm (moot); 8:00pm (awards ceremony)

Venue: Auckland High Court, Cnr Waterloo Quadrant & Parliament Streets

Members of the profession are warmly invited to attend the final, and should RSVP to laweventsauckland.ac.nz. LN

+ LinkedIn book

LinkedIn for Lawyers: Connect, Engage and Grow Your Business, 2nd Edition

Author: Kirsten Hodgson

NEW EDITION DUE IN AUGUST 2015

Stop thinking about LinkedIn as a social network, and start thinking about it as a marketing network. LinkedIn is a powerful tool in an ever-changing online landscape, and can be effectively leveraged to help achieve business development and marketing goals.

This practical guide is a thorough update to the first edition of *LinkedIn for Lawyers: Connect, Engage and Grow Your Business*, and is a vital resource for any lawyer who wants to take advantage of the marketing and business development opportunities offered by LinkedIn.

This book provides guidance and practical examples on how to:

- build and raise your profile;
- manage your reputation;
- build your knowledge base and keep up-to-date with key issues in your area(s) of expertise;
- position yourself as an expert in your field;
- generate new business;
- keep in touch with, and engage with, your existing clients and referrers;
- research clients, prospects and competitors;
- meet and engage with prospects, potential referrers, colleagues and peers; and
- get the right people into your sales funnel.

This updated edition also includes a "lightning reference guide" to leveraging other social media for your business, including Facebook, Twitter and Pinterest.

Price: $47.83 plus GST ($55.00 incl. GST)*

Price for ADLSI Members: $43.04 plus GST ($49.50 incl. GST)*

(+ Postage and packaging)*

To purchase this book, please visit www.adls.org.nz/adlsi-store or contact the ADLSI bookstore by phone: 09 306 5740, fax: 09 306 5741 or email: thestore@adls.org.nz.