LexisNexis

# Internet Law Bulletin

2016 . Vol 19 No 2

## Contents





*Information contained in this newsletter is current as at March 2016*

LexisNexis Butterworths

# The Hague Conference's "Judgments Project" 2.0 — how will it work in relation to e-commerce?

***Dr Dan Jerker B Svantesson*** *BOND UNIVERSITY*

## Introduction

The Hague Conference on Private International Law (Hague Conference) has been working to harmonise and improve the application of the rules of private international law for more than 100 years. Some of the recent successes include the Hague Convention on Choice of Court Agreements (the Convention), concluded on 30 June 2005, and the Hague Principles on Choice of Law in International Commercial Contracts, approved on 19 March 2015.

In 1992, work on a new and ambitious convention was initiated at the Hague Conference. However, due to a range of factors, not least its wide scope, the great ambitions of the Judgments Project (as it was referred to) proved impossible at the time. When the work on the Judgments Project was first initiated, little regard was given for the special needs created by the internet. However, it soon became apparent that the internet raised several complex issues that made the finalising of the Judgments Project more difficult. At the same time, the widespread use of the internet amplified the importance and necessity of international instruments like the previously proposed Convention.

In recognition of the importance of the project, the Hague Conference has now resumed work on the Judgments Project. A report issued by the Council on General Affairs and Policy of the Conference in April 2011 breathed new life into the project.[1] This marked the start of renewed efforts driving the Judgments Project forward. The outcome of this work is found in the report of the fifth meeting of the working group on the Judgments Project (26–31 October 2015) with a proposed draft text resulting from the meeting.[2]

The Convention is a significant initiative with the potential to provide real benefits. The structure and approach adopted, as well as of the goals pursued are generally sound. However, as can be expected, some additional work is needed.

In this brief article, I will analyse some of the key features of the proposed draft text with particular emphasis on how the text will work in the context of the internet and e-commerce.

## The over-all purpose

The Convention is aimed at meeting real, practical needs which are not met by existing instruments and institutional frameworks. It will enhance access to justice and facilitate trade and investment. The over-all purpose of the new proposal is made clear in Art 4, which clearly is the most important part of the proposal:[3]

> A judgment given by a court of a Contracting State (State of origin) shall be recognised and enforced in another Contracting State (requested State) in accordance with the provisions of this Chapter. Recognition or enforcement may be refused only on the grounds specified in this Convention.

There can be no doubt that there is a need for improved procedures for the recognition and enforcement of foreign judgments, and the increase in cross-border interaction sparked by the internet is an important reason for that need. At the same time, we must not lose sight of the fact that enforcement difficulties paradoxically are important for the functioning of the internet — just imagine if every law of every country in the world was enforced against any content you post online. Would we, for example, wish for the restrictive laws of the world's dictatorships to be enforced globally? What would be left online? Not much.

Thus the reality is that, while the goals of the proposed Judgments Project are commendable as such, it is crucial that appropriate restrictions are placed on the situations in which foreign judgments are recognised and enforced under the Convention.

## The scope of the proposed Convention

Article 1 of the Proposed Draft Text emphasises that the Convention applies between Contracting States and that it is focused on the recognition and enforcement of judgments relating to civil or commercial matters. Under Art 2, several areas, including the carriage of passengers and goods, arbitration and defamation, are excluded from the scope of the Convention. Importantly, while the February 2015 preliminary text specifically pointed out that:[4]

> [f]urther consideration is needed of the proposals made to include specific provisions for recognition and enforcement of certain consumer and employment judgments.

The October 2015 proposed draft text includes both consumer contracts and employment contracts.[5]

Of particular relevance, Art 2(1)(k) excludes defamation from the scope of the Convention. While such an exclusion has both advantages (eg, avoiding having to tackle a particularly controversial area) and disadvantages (eg, a missed opportunity to tackle a particularly controversial area), it is difficult to see why judgments rendered in defamation disputes are excluded if judgments rendered, for example, in data privacy disputes are not.

In other words, if there is a commitment to excluding defamation, it is necessary to carefully consider whether to also exclude other areas of law — such as data privacy and breach of confidence — that share fundamental characteristics with defamation. In particular, data privacy is emerging as an area of huge importance, and (not least given that Art 2(5) caters for the enforcement of judgments in dispute to which governmental agencies are parties) the status of data privacy judgments must be carefully considered, both in the context of Art 2(1)(k) and in the context of Art 1(1) referring to "civil or commercial matters".[6]

In this context, mention may be made of the approach taken in the EU's Rome II Regulation, in which "non-contractual obligations arising out of violations of privacy and rights relating to personality, including defamation" are excluded.[7] This wording may perhaps be "too European" for an international convention, and the exclusion has been controversial and may not be maintained long-term.[8] However, as an approach to delineating the excluded areas, it may be better suited than simply making reference to defamation, unless of course there are specific reasons for excluding defamation while still including closely related areas.

## The grounds for jurisdiction that result in a duty to recognise and enforce

Article 5 outlines the grounds for jurisdiction that result in a duty on other Contracting States to recognise and enforce the judgment of the original court. Most of these grounds are both predictable and generally sensible. For example, a judgment is eligible for recognition and enforcement if the person who was the party in the proceedings in the court of origin and is the person against whom recognition or enforcement is sought was habitually resident in the state of origin at the time that person became a party to the proceedings in the court of origin.

Others, not surprisingly, will benefit from detailed consideration when applied in the internet and e-commerce setting. Article 5(1)(c) provides that:[9]

> A judgment is eligible for recognition and enforcement if … the defendant maintained a branch, agency, or other establishment without separate legal personality in the State of origin at the time that person became a party to the proceedings in the court of origin, and the claim on which the judgment is based arose out of the activities of that branch, agency, or establishment;

However, in the context of e-commerce, the question of what level of activity is required for the conclusion that the defendant maintains an "establishment" in the state of origin needs careful consideration and it should not be assumed that different states will apply the same test for this.[10]

Another provision that needs special consideration from an e-commerce perspective is Art 5(1)(e). That Article makes clear that:[11]

> A judgment is eligible for recognition and enforcement if … the judgment ruled on a contractual obligation and it was given in the State in which performance of that obligation took place or should take place under the parties' agreement or under the law applicable to the contract, unless the defendant's activities in relation to the transaction clearly did not constitute a purposeful and substantial connection to that State;

However, ascertaining where the performance of certain e-commerce obligations take place or should take place is notoriously difficult and can only be done by reference to legal fictions. For example, where does the performance take place where a person who lives in State A part of the year, but who spends part of the year in State B and works in and spends a lot of time in State C, subscribes to an online streaming service? In light of this type of difficulty, the wisdom of placing reliance on such a concept is questionable unless more guidance is provided.

## The particular position of consumer contracts

The proposed text contains special rules for consumer contracts. However, the term "consumer" is not defined. This may cause complications as not all countries define that term in the same manner. For example, under the Australian Consumer Law, the special protection afforded to consumers extends to certain business-to-business (B2B) contracts where the business essentially is in the same position as a consumer would be in the contractual situation in question. Thus, as I have stressed in the context of the 2005 Hague Convention,[12] given Australia's comparatively broad definition of consumers, there is a mismatch between what is dealt with as consumers under Australian law and what is likely to be treated as

consumers under the Convention. It would be inappropriate for the Convention to result in a narrower consumer protection in Australia.

At any rate, the special rules protecting consumers state that, where recognition or enforcement is sought against a consumer in matters relating to a consumer contract, reliance on jurisdiction based on the defendant's consent (as provided for under Art 5(1)(d)) applies only if the consent was given before the court, and jurisdiction may not be based on the location of actual or anticipated performance (as provided for under Art 1(e)). The end result of this is that, as far as consumers are concerned, the main jurisdictional basis upon which judgments may be recognised and enforced under the Convention is jurisdiction based on the consumer's habitual residence. This thinking is in line with that of the EU's Brussels I bis Regulation[13] which ensures that consumers, in certain situations, only may be brought before the courts of their home state. However, two differences ought to be emphasised. First, the approach taken in the proposed Convention text applies to all consumer contracts, and second, unlike the Brussels I bis Regulation, the proposed convention text does not give the consumer the right to always pursue the other contractual party in the consumer's home state.

## The particular position of intellectual property judgments

Judgments relating to intellectual property disputes enjoy a special status under the proposed convention. Article 5(1)(g) and (h) deal with the jurisdictional grounds for intellectual property disputes. Such a judgment is eligible for recognition and enforcement if:[14]

> g) the judgment ruled on an infringement of a patent, trademark, design or other similar right required to be deposited or registered and it was given by a court in the State in which the deposit or registration of the right concerned has taken place;
> h) the judgment ruled on the validity or infringement of copyright or related rights and the right arose under the law of the State of origin;

In addition, Art 6 adds that:[15]

> Notwithstanding Article 5 —
> a) a judgment that ruled on the registration or validity of patents, trademarks, designs, or other similar rights required to be deposited or registered shall be recognised and enforced if and only if the State of origin is the State in which deposit or registration has been applied for, has taken place, or is deemed to have been applied for or to have taken place under the terms of an international or regional instrument;

As is illustrated by the work of the International Law Association's Committee on Intellectual Property and Private International Law,[16] it is doubtful that Art 5(1)(g) and (h) adequately address the complexities of that area. Pursuing this topic further here would, however, take us too far afield.

## The need to consider "scope of jurisdiction"

Article 9 looks to the nature of damages awarded by the original court, and caters for the refusal to recognise and enforce judgments to the extent the judgment awards damages, including exemplary or punitive damages, that do not compensate a party for actual loss or harm suffered. This is appropriate. However, similar concerns may arise in relation to other types of remedies. For example, there is a tendency at the moment for courts to be saying that the only way one can comply with an order to remove access to internet content in their country is to remove the content globally. Where that approach is taken, there should be the option to refuse to recognise and enforce the judgment.

This connects to a bigger issue that the proposed Convention usefully could take account of — a matter I have referred to as "scope of jurisdiction".[17] Scope of jurisdiction relates to the appropriate geographical scope of orders rendered by a court that has personal jurisdiction and subject-matter jurisdiction. Whether or not a court ought to recognise and enforce a foreign judgment depends, in part, on whether the court rendering the judgment has made a ruling with an appropriate geographical scope. This is a question that only will grow in importance, not least in the internet context, and should not be overlooked in a forward-looking document such as the proposed Convention.

## Translation — a serious barrier to recognition and enforcement

Article 11(4) states that if the documents that need to be produced by the party seeking recognition and enforcement (including, eg, a complete and certified copy of the judgment) are not in an official language of the requested state, they shall be accompanied by a certified translation into an official language, unless the law of the requested state provides otherwise.

The translation requirement outlined in Art 11(4) will effectively work as a cost-based barrier to the recognition and enforcement of judgments in some situations; that is, if the costs of the translation exceed the potential gain from having the judgment enforced, people will not pursue enforcement. This barrier may well be intentional and, in any case, may be difficult to avoid; but its implications should be expressly acknowledged.

## Concluding remarks

The Judgments Project 2.0 is a timely and generally well-considered initiative, and the Hague Conference

deserves to be congratulated for resurrecting this ambitious project with its huge potential for improving cross-border recognition and enforcement. The draft text produced is a great starting point, and the fact that it needs further refinement cannot be seen as a flaw; it is a both natural and necessary feature of a draft text addressing a complex area.

In moving forward towards a final text, it would be useful to subject the draft text to a careful and detailed "Impact of Internet Technology Assessment" — a detailed study of how well the provisions of the draft text work when applied in internet-related scenarios.

In any case, there can be no doubt that the Judgments Project brings attention to an important area of tremendous practical importance — an area to which lawyers perhaps devote insufficient attention. Thus, lawyers are well advised to monitor the Judgments Project's developments.

## Tips for lawyers:

- The actual enforcement of any orders sought must be at the forefront from the start of litigations.
- Especially online, most disputes have an international dimension. This can work to your advantage if you understand the international system, or it can be seen as a risk if you do not.
- The work of international bodies such as the Hague Conference on Private International Law ought to be monitored constantly.
- In fact, given the impact the proposed Convention will have, the Australian legal community is well advised to take an active interest in how the Convention develops.

***Dr Dan Jerker B Svantesson***
*Professor and Co-Director*
*Centre for Commercial Law, Faculty of Law*
*Bond University (Australia)*
*Researcher*
*Swedish Law & Informatics Research Institute*
*Stockholm University*
*Dan_Svantesson@bond.edu.au*

*Professor Svantesson is the recipient of an Australian Research Council Future Fellowship (project number FT120100583). The views expressed herein are those of the author and are not necessarily those of the Australian Research Council.*

## Footnotes

1. The Hague Conference on Private International Law, *Council on General Affairs and Policy of the Conference, Conclusions and Recommendations of the Council on General Affairs,* (2011), www.hcch.net.
2. The Hague Conference on Private International Law, *Report of the Fifth Meeting of the Working Group on the Judgments Project (26–31 October 2015) and Proposed Draft Text Resulting from the Meeting,* (2015), www.hcch.net.
3. Above n 2, at ii.
4. The Hague Conference on Private International Law, *Report of the Fourth Meeting of the Working Group on the Judgments Project (3–6 February 2015) and Preliminary Draft Text Resulting from the Meeting,* (2015), www.hcch.net.
5. Above n 2, at 4.
6. For a discussion of data privacy and private international law specifically, see eg, M Brkan "Data Protection and European Private International Law: Observing a Bull in a China Shop" (2015) 5(4) *International Data Privacy Law* 257–78.
7. Official Journal of the European Union, *European Parliament resolution of 10 May 2012 with recommendations to the Commission on the amendment of Regulation (EC) No 864/2007 on the law applicable to non-contractual obligations (Rome II) (2009/2170(INI))* (2012). See http://eur-lex.europa.eu
8. See eg, D Svantesson "The Rome II Regulation and choice of law in Internet-based violations of privacy and personality rights — on the wrong track, but in the right direction?" (2011, published 2014) 16 *Austrian Review of International and European Law* 275–97.
9. Above n 2, at iii.
10. See eg, the discussion in the recent EU *Weltimmo* case Case C-230/14.
11. Above n 2, at iii.
12. D Svantesson "The Choice of Courts Convention — How will it work in relation to the Internet and e-commerce?" (2009) 5(3) *Journal of Private International Law* 517–35.
13. Official Journal of the European Union *Council Regulation (EC) No. 1215/2012, 12 Dec. 2012, on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast)* (2015).
14. Above n 2, at iii.
15. Above n 2, at iv.
16. International Law Association, *Intellectual Property and Private International Law,* (2008), www.ila-hq.org.
17. D Svantesson "Jurisdiction in 3D — 'scope of (remedial) jurisdiction' as a third dimension of jurisdiction" (forthcoming April 2016) *Journal of Private International Law*.

# The revision of the Evidence Act 1929 (SA) to account for the treatment of electronic communications as evidence

***Gabriella Shailer*** *UNIVERSITY OF ADELAIDE*

## Takeaway points

- Once commenced the Evidence (Records and Documents) Amendment Act 2015 (SA)[1] (the Act) will amend the Evidence Act 1929 (SA) to reflect the provisions of the Evidence Act 1995 (Cth) relating to electronic communications.
- The amendments will create a rebuttable presumption that the origin and destination, the timing and the parties to the communication are accurate. The hearsay rule will not be applicable to any or all of this information.
- The amendments will modify the best evidence rule to allow a representation of electronic intelligence that does not include the supporting code (such as a screen shot) to be entered into a proceeding as evidence.

## Introduction and overview

The Evidence (Records and Documents) Amendment Act 2015 (SA) (the Act)was introduced into the South Australian Parliament in October 2015. The main objective of the Act was the creation of a uniform set of rules surrounding the admittance of electronic communications as evidence in a legal proceeding. The impetus for the amendments was to remove the ad hoc and inconsistent treatment of electronic communications as evidence by creating an efficient and effective set of legislative rules.[2] Once the amendments commence, the treatment of electronic communications as evidence will be consistent with the Evidence Act 1995 (Cth) (Evidence Act 1995).

This article will discuss several of the pending amendments to the Evidence Act 1929 (SA) (Evidence Act 1929) that are relevant for the consideration of electronic communications data as evidence in a legal proceeding. In particular it will consider the effects of the creation of the rebuttable presumption that electronic communication records are accurate including the creation of an additional exception to the hearsay rule. The article will provide a brief overview of background, a descriptive scope of the statutory obligations on the practitioner and provide comment on the potential effects of the change.

## Background

The Australian Communications and Media Authority (ACMA) continue to acknowledge a trend towards utilisation of online services as the primary means of communication between citizens.[3] However there are no explicit rules governing the admittance of electronic telecommunications data as evidence within the South Australian jurisdiction.[4] As a result the electronic records are not admitted into evidence on consistent terms. Cognoscente of this The South Australian Law Reform Institute (SALRI) produced a report called *Modernisation of South Australian evidence law to deal with new technologies* (*Modernisation Report*) in 2012. The *Modernisation Report* detailed recommendations for the treatment of a body of evidence of communications data such as personalised profiles, public and private messages and blogs that will be central to proceedings moving forward. The recommendations are consistent with the treatment of electronic communications in the Evidence Act 1995.[5] The recommendations from the *Modernisation Report* were used as a basis for the amendments proposed in the Bill.

## Statutory text

The aim of the statutory scheme is to create a uniform set of rules that would account for the admittance of electronic communications as evidence. This is primarily achieved when the Act inserts s 56 into the Evidence Act 1929. Section 56 creates a rebuttable presumption that electronic records are as they appear. The Act will insert ss 54 and 57 into Evidence Act 1929 that act in support of s 56. Section 54 creates a rebuttable assumption that metadata type details including the origin and time of the communication are as they appear. Section 57 defines the circumstances under which a reasonable reproduction of data may be introduced into evidence. Sections 54 and 57 will be discussed in more detail below.

The Act is designed to address the treatment of electronic communications as evidence. It inserts the definition of electronic communications from the Electronic Transactions Act 2000 (SA); which is:

> (a) a communication of information in the form of data, text or images by means of guided or unguided electromagnetic energy, or both; or
> (b) a communication of information in the form of sound by means of guided or unguided electromagnetic energy, or both, where the sound is processed at its destination by an automated voice recognition system.

The proposed definition is consistent with the definition in the Electronic Transactions Act 1999 (Cth). The wording of the definition gives a targeted definition of electronic communications. It goes some way to future proofing the definition for developments in technology, as it does not discriminate on the particular type of technology or the device utilised to construct the communication. The broad scope of the definition is consistent with submissions to the review of the same in the Evidence Act 1995 which concluded that limitation on terms including "electronic mail" or "electronic commerce" would render the legislation redundant as technology progressed.[6]

The Act has responded to the recommendation to simplify the rules for the admittance of electronic data as evidence in the *Modernisation Report*. It deletes the existing statutory requirements for the admittance of electronic evidence in s 6A. The *Modernisation Report* concluded that s 6A was redundant, noting it was created before mainstream usage of the internet and the tests contained within s 6A were rarely applied in proceedings.[7] The *Modernisation Report* noted a conflict with s 6A and the more recently created tests of a similar nature in the Uniform Evidence Act.[8]

The Act will insert s 56 which replaces the tests in s 6A. Section 56 creates an assumption that electronic data is "as it appears". The primary purpose of s 56 is to alter the burden of proof as it relates to the authenticity of the evidence. This was intended to create efficiencies in proceedings. The requirement to authenticate all electronic communications data is regarded as a needless formality. This is because a substantial volume of documentary evidence is created by computer systems in contemporary Australia and errors within systems are not commonplace. The *Modernisation Report* concluded it would be more efficient for the practitioner asserting the error in the data to provide evidence of the problem.[9]

The Act will insert s 57 into the Evidence Act 1929. Section 57 modifies the s 45C best evidence rule. It allows reproduced evidence in either the same format or a different format as the original into evidence. Section 57 specifically references introducing a screen shot as a reasonable reproduction of social media evidence. In doing so, it allows electronic communications to be introduced as evidence without the supporting code.

Section 54 of the Act creates a rebuttable presumption that the origin, destination, source, timing and identity of the sender and recipient are accurate. The hearsay rule may not apply to what is represented in a document recording an electronic communications if the question of fact relates to any of the element of the rebuttable presumption as documented in s 54. Section 54 is modelled on ss 71 and 161 of the Uniform Evidence Act.

The scope of s 54 is not limited to communications that happen within the bounds of the Australian Commonwealth. The removal of the jurisdictional limitation on the communication will remove administrative problems that will inevitably occur when a site that is hosted overseas generates or hosts communications data. This provision will also assist in instances where data may be categorised as "foreign" data because it has travelled a route that includes a node outside of the geographic reach of the Commonwealth of Australia. This is a frequent occurrence. For example, telecommunications companies that are intrinsically Australian, such as Telstra, commonly store telecommunications data in overseas data centres.[10] It is also common for communications including SMS to be routed outside of the continental bounds of the sender and recipient.[11]

## Observations

The amendments documented in the Act reflect a genuine attempt to engage with the technology that will govern the treatment of electronic data as evidence.[12] The drafters have considered the intention of the recommendations from the *Modernisation Report* and enacted these where possible. The *Modernisation Report* reasoned that the rules in s 6A were overly burdensome and concluded that it would be more efficient for the practitioner seeking to assert a deficiency to prove the existence of that error. The amendments documented in the Act propose an alternative statutory scheme that appreciates the practical authentication requirements of the data to be entered as evidence. The almost impossible requirement to prove that the device was functioning without error at the time the data was created has been removed. The onus of proving an error with the data is now placed on the individual asserting the issue. This creates efficiency as it is comparatively simpler to prove the error in the cases where the reliability of the data is in question than to prove the absence of errors in every situation where electronic data is called into evidence.

The proposed revision of the definition of electronic communications is not merely an adaption of the historical definition of communications. There has been some attempt to engage with technology and common usage.[13] The specific wording is not device or technology specific and therefore has the capacity to evolve with technology. This will create efficiencies for the legal practitioner by removing artificial limitations within the definitions that would affect the application of the rules moving forward.

However, it is arguable that some elements of the Act do not appreciate the realities of the technological landscape. For example, the separation of the content from the code in an official capacity is potentially risky in a legal proceeding. The action is arguably more relevant for social media data because the capacity and motivation to augment metadata type details of specific elements of data is already well documented. For instance, Carina Santos is a social bot created by academics at the Federal University of Ouro Preto in Brazil. It was able to earn the same online influence as Oprah Winfrey in its immediate geographic area over the 2 years it was running.[14] The 2015 hack on *Avid Life Media's Ashley Madison* dating profile showed that an overwhelming percentage of the "women" on the site where inactive shop front style personas that were entered by employees or social bots.[15] Similarly, the literature explaining how to generate "fake" metadata associated with a social media communication is easily available online[16] to the point where businesses such as Please Don't Stalk Me offer services such as the ability to send a tweet from anywhere in the world.[17]

These examples show the ease and the scale at which key details of communications can be faked. The location of the individual may be a key element of a proceeding. The code may be essential to assessing the credibility of the evidence. The amendments will allow a practitioner to enter evidence without the supporting code. The opposing practitioner may not be in a position to challenge the presumption of accuracy if the code cannot be accessed. There is a strong possibility that the code may not be reasonably available. The major telecommunications providers have already asserted no intention to retain data outside of the existing legislative obligations; instead opting to delete on business efficacy grounds.[18]

In order to minimise the risks associated with the creation of a telecommunications hearsay exception as drafted the practitioner would need to be able to access business records from companies outside the Australian jurisdiction which will not be possible in all instance. This will stop the presumption of accuracy being challenged but not the ability to enter the data as evidence; which in turn creates a risk that the result of proceedings may be influenced by factually inaccurate data.

## Conclusions

The proposed amendments to the Evidence Act 1929 were essential in the contemporary Australian environment. The continued reliance on computer systems necessitated a need to create a uniform set of rules governing the treatment of telecommunications data as evidence in a legal proceeding. The major contribution of the Act is the creation of the assumption that electronic communications data is accurate. The onus of proof is on the party asserting an issue with authenticity of data. This will promote efficiency within the profession as it is comparatively simpler to prove a problem than the absence of one.

However, it is arguable that the drafters of the Act have not appreciated the impact of technology on the law in all instances. The major point of concern highlighted in this article is the creation of the assumption that telecommunications data is "as it appears". The assumption creates the capacity to enter electronic communications data such as social media data into evidence without the need to associate the supporting code. The problem stemming from this methodology is that the opposing legal practitioner may require the code to prove the error in the data and the code may not be available. If this is the case then legal proceedings may be decided on the basis of factually inaccurate data.

***Gabriella Shailer***
*BA Interior Architecture, Curtin University*
*JD, Murdoch University*
*PhD Candidate, University of Adelaide*

*The author would like to thank Professor Melissa De Zwart, University of Adelaide, for her assistance with this article.*

## Footnotes

1. The Evidence (Records and Documents) Amendment Act 2015 (No 39 of 2015) will come into operation on 4 April 2016. See Gazette No. 6, 4/2/2016, p 366
2. South Australia, *Parliamentary Debates*, House of Assembly, 28 October 2015, (Gail Gago).
3. Australian Communications and Media Authority *Communications Report 2013–2014* (2014) p 4.
4. South Australian Law Reform Institute *Modernisation of South Australia's Evidence Law to deal with New Technologies* Final Report 1 (2012) para 2.9.

5. Above n 4, at para 2.8.
6. Australian Law Reform Commission *Review of the Uniform Evidence Acts* Discussion Paper 69 (2005) 151.
7. Above n 4, at para 2.14.
8. Above n 4, at para 2.15.
9. The requirement to authenticate every electronic communication was considered burdensome given the high volume of electronic communications that occur in contemporary Australia. See above n 4, at para 2.16.
10. Telstra, *Colocation, A cost-effective and highly secure solution to your data housing needs,* www.telstraglobal.com.
11. J Oliver, *Government Surveillance - Last Week Tonight* (5 April 2015) available at www.youtube.com.
12. Above n 4, at Recommendations.
13. The *Modernisation Report*/Bill referenced the research completed by the ALRC to come to the definition of electronic communication. This included consultation with the legal industry. See above n 6, at 150.
14. Urbina I "I Flirt and I Tweet. Follow me at #socialbot" *The New York Times* 10 August 2013, www.nytimes.com.
15. A Newitz, *How Ashley Madison hid its Fembot Con from its users*, August 2015, www.gizmodo.com.
16. S Haider, *How To: Geotag Fake Locations on your Twitter Tweets,* March 2013, www.shaanhaider.com; Revision3, *Fake your Tweet Location!*, December 2012, www.revision3.com; A Agarwal, *Geotag your Tweets with any Random Location,* November 2012, www.labnol.org.
17. See www.pleasedontstalkme.com.
18. R Chirgwin, *Telstra, Vodafone at odds over Data Retention,* September 2014, www.theregister.co.uk.

# New report compiled by the Association of Corporate Counsel Foundation — The State of Cybersecurity Report: an in-house perspective

***Julian Lincoln*** *and* ***David Miller*** *HERBERT SMITH FREEHILLS*

## Key takeaways

- The Association of Corporate Counsel Foundation has published *The State of Cybersecurity Report: an in-house perspective*.
- The *Report* seeks to analyse the state of cybersecurity from an in-house lawyer perspective.
- There are a number of important findings, including that almost one in three in-house lawyers experienced a data breach at their organisation.
- The *Report* builds on a growing body of research regarding cybersecurity from a legal perspective, including previous work of the Association of Corporate Counsel Foundation.

## The ACC Report

In December last year, the Association of Corporate Counsel Foundation (ACC) published the *State of Cybersecurity Report: an in-house perspective*, underwritten by US law firm Ballard Spahr LLP (*Report*). The *Report* comprises a survey of senior corporate lawyers from 30 countries, and seeks to analyse the state of cybersecurity from an in-house legal perspective.[1]

The full *Report* is available for purchase on the ACC website.

The ACC notes that the full *Report* includes:[2]

- industry and regional trends;
- common preventative tactics;
- lessons learned from those who experienced a breach (including how the breach occurred and who was affected);
- the impact of regulatory requirements;
- insurance decision making and coverage information; and
- managing risk through outside support such as forensic and outside counsel retainers, [as well as other matters].

The survey opened on 31 August 2015 and closed on 10 October 2015. The ACC sent an email invitation to participate to 15,176 chief legal officers, general counsel and assistant general counsel. Of the total 1015 responses received, 77% identified as general counsel or chief legal officer and 14% as assistant general counsel, with the remainder holding other in-house legal titles.

The *Report* builds on a growing body of research regarding cybersecurity from a legal perspective, including a recent census also conducted by the ACC of more than 5000 in-house lawyers in 73 countries. The census found that in-house lawyers considered cybersecurity one of the greatest compliance challenges, just behind privacy, which ranked as the number one compliance challenge.[3]

While the *Report* provides a global view, further Australian specific research is available. The *Report* cites the recent Ponemon Institute *Cost of Data Breach Study: Global Analysis* which found that, in Australia, the average cost of a data breach for companies in the study was AUD $2.8 million, including the cost of lost business and customer churn.[4] Importantly, in its latest annual report the Office of the Australian Information Commissioner reported receiving 110 voluntary data breach notifications for 2014–15, which represents an increase of 64% on the previous year.[5]

## Key findings of the Report

The ACC have made the key findings of the *Report* available on the ACC website.[6] Some of the key findings include:[7]

### *Increasing reality of data breaches*

- Almost one in three in-house lawyers experienced a data breach at their organisation.
- 45% of in-house lawyers in companies with 5000 or more employees reported that they either work, or have worked, at a company that experienced a data breach.
- 19% reported that their current organisation experienced a data breach, while 10% reported that their former employer/organisation experienced a data breach.

### *Increasing legal spend*

- There is a clear increase in budget allocation toward cybersecurity.

- 56% of general counsels/chief legal officers reported an increase in budget allocation for cybersecurity on 2014, and 23% reported their overall legal department spend has increased as a result of an enterprise-wide focus on cybersecurity generally.
- Of those reporting an increase in spend, 53% reported the increase is mainly outside spend (ie, external lawyers) and 24% reported the increase as equally split between internal and outside spend.

### *Industry trends*

- There are emerging industry trends regarding data breaches.
- 56% of in-house lawyers in the healthcare/social assistance industry reported experiencing a data breach, 36% in the insurance industry, 33% in the manufacturing industry, 32% in the retail industry and 31% in the IT/internet services industry.

### *Evolving role of the lawyer*

- 50% of all general counsels/chief legal officers reported a desire to increase their roles and responsibilities regarding cybersecurity.
- While oversight of cyber-risk continues to sit primarily with the IT department, the legal role is expanding with 57% of general counsels/chief legal officers expecting their department's role to increase in the coming year.

### *Rise of cyber insurance*

- Half of all general counsels/chief legal officers reported that their organisation has cybersecurity insurance, and 68% of these organisations reported coverage valued at USD 1 million or more.
- One in four surveyed reported an expectation that their organisation would increase cybersecurity insurance coverage in the coming year.

The full *Report*, as well as further information about the *Report* and the ACC generally, is available on the ACC website.[8]

***Julian Lincoln***
*Partner*
*Herbert Smith Freehills*
*Julian.Lincoln@hsf.com*

***David Miller***
*Solicitor*
*Herbert Smith Freehills*
*David.Miller@hsf.com*

*For information regarding cybersecurity and legal compliance in Australia, contact Julian Lincoln, Partner at Herbert Smith Freehills or David Miller, Solicitor at Herbert Smith Freehills.*

## Footnotes

1. See Association of Corporate Counsel *ACC Foundation: the State of Cybersecurity Report* (2009) www.acc.com.
2. See Association of Corporate Counsel *Key Findings from the ACC Foundation: the State of Cybersecurity Report* (2015) www.acc.com.
3. See Association of Corporate Counsel *2015 ACC Global Census* (2015) www.acc.com.
4. See Ponemon Institute *2015 Cost of Data Breach Study: Australia* (2015) www.public.dhe.ibm.com.
5. See Office of the Australian Information Commissioner *Annual Report 2014–15* (2015) www.oaic.gov.au. Note also that in December 2015 the Australian Government issued an exposure draft bill for mandatory data breach notification for public consultation.
6. Above n 2.
7. Above n 2, at p 6.
8. Above n 1.

# The blurred lines between blogging and business: a case analysis of Fletcher v Nextra Australia Pty Ltd

***Stephanie Hayes***

## Introduction

"Blogs" are typically viewed as an avenue for personal expression as well as a means for engaging in popular debate, and the relative informality of such sites might lead "bloggers" to assume that their activities are immune to the operation of consumer law. However, in April this year, the Full Court of the Federal Court decided in *Fletcher v Nextra Australia Pty Ltd*[1] that an individual who had published an article on a privately operated blog had engaged in misleading or deceptive conduct "in trade or commerce" pursuant to s 18 of the Australian Consumer Law (ACL). The decision serves as a useful reiteration of the principles expounded by the High Court in C*oncrete Constructions (NSW) Pty Ltd v Nelson (Concrete Constructions)*,[2] while at the same time highlighting the evaluative process that must be undertaken to distinguish between those types of conduct that may, or may not, prompt the operation of s 18.

## Facts

Mr Fletcher published an article (the article) on his self-operated Australian Newsagency Blog (the blog) in which he criticised a promotional flyer that had been circulated by Nextra Australia Pty Ltd (Nextra). While the blog was operated in his personal capacity, Mr Fletcher was also a director and 50% shareholder of newsXpress Pty Ltd (newsXpress), a competitor of Nextra in the national news agency franchise market. Nextra alleged that the publication of the article constituted misleading or deceptive conduct in trade or commerce in contravention of s 18 of the ACL.

## Decision at first instance

In order to establish a contravention of s 18 of the ACL, it must be shown that:

1. the conduct is misleading or deceptive or is likely to mislead or deceive; and
2. the conduct occurred in trade or commerce.

A single justice of the Federal Court ***decided at first instance*** that at least one of the imputations made in Mr Fletcher's article was a false representation of fact, thereby satisfying the first limb of s 18. The case thus primarily centred upon the second limb — the question of whether the conduct had occurred in trade or commerce. In making that assessment, Collier J applied the test set down by the High Court in Concrete Constructions. That case concerned s 52 of the Trade Practices Act 1974 (Cth) — the predecessor to s 18 — and remains a leading authority on the interpretation of the phrase "in trade or commerce". Mason CJ and Deane, Dawson and Gaudron JJ held that, in order to determine liability, "the central conception" of trade or commerce must be distinguished from "the 'immense field of activities' in which corporations may engage in the course of, or for the purposes of, carrying on some overall trading or commercial business".[3]

Collier J thus examined the essential character of Mr Fletcher's blog and the role, if any, it had to play in promoting the commercial interests of newsXpress. Mr Fletcher explained that his extensive experience in the news agency industry meant he was a voice of influence, and that the blog was used to facilitate information-sharing and discussion among his fellow industry participants. While Collier J accepted that Mr Fletcher's non-commercial interest in doing so was genuine, her Honour pointed to earlier publications on the site which demonstrated that the blog went beyond the mere ventilation of Mr Fletcher's personal opinion. The court found that Mr Fletcher had used the blog to discuss (and thereby promote) the commercial interests of newsXpress, a point which resonated with the facts in *Universal Music Australia Pty Ltd v Cooper*.[4] The respondent in that case had used free music files to entice internet users to visit his website. The availability and accessibility of the files generated a commercial benefit for Mr Cooper in the form of sponsorship and advertising revenue, thus forming a "central conception" of his business activity.[5] While Mr Fletcher's blog was not published on behalf of newsXpress, its target audience included those whose business decisions might be affected by the content delivered on the site. The court

held that the article was not independent commentary but rather an attempt to protect newsXpress by preventing Nextra from "poaching" franchisees. Thus, the court concluded that "[t]he posting of the Article by Mr Fletcher was not conduct divorced from his relevant actual or potential trading or commercial relationships, as envisaged in *Concrete Constructions*.[6]

Mr Fletcher was ordered to remove the article from the blog and was restrained from publishing it in any other form.

## Decision on appeal

Mr Fletcher appealed the decision on the basis that there was insufficient evidence to establish that the publication of the article was essentially designed to protect the commercial interests of newsXpress. Even if the blog *did* have that fortuitous effect, Mr Fletcher argued that alone was insufficient to meet the test in *Concrete Constructions*. In that regard, he relied particularly on the observation of French, Sackville and Conti JJ in *Village Building Co Ltd v Canberra International Airport Pty Ltd*[7] where their Honours said:[8]

> The fact that conduct has the purpose or effect (or both) of maintaining or protecting a business is not, of itself, enough to ensure that the conduct is in trade or commerce.

Mr Fletcher thus argued that the requirement, articulated by Collier J, that his conduct be "divorced"[9] from his trading or commercial relationships heralded an impermissible extension of the test laid down in *Concrete Constructions*. In any event, Mr Fletcher denied that the article was intended to promote the commercial ventures of newsXpress[10] — a distinction which, he asserted, meant that his conduct could not be characterised as having occurred in trade or commerce for the purposes of s 18.

The Full Court rejected Mr Fletcher's appeal. Middleton, McKerracher and Davies JJ evaluated *the character of the conduct* by reference to what their Honours regarded to be the key elements of the case, which included that:[11]

> — Mr Fletcher appreciated the status and authority that the publication of the Blog of this nature conferred on him in the newsagency community;
> — Mr Fletcher had not previously hesitated to use the Blog to promote his own commercial interests;
> — the Article is an example of Mr Fletcher using the Blog for commercial purposes, namely, to promote newsXpress…; and
> — the posting of the Article was for the purpose of defending newsXpress from what he saw as potential poaching of franchisees by Nextra.

Their Honours ultimately concluded that Mr Fletcher's conduct was analogous to that of conventional comparative advertising, whereby advertisers make assertions about the inadequacies of their competitors' products. The Full Court observed that it "has never been doubted that such advertising is conduct in trade or commerce".[12] Mr Fletcher's active participation in the news agency franchise industry, together with the fact that his conduct was intended to have an impact on trading or commercial activities, fortified that conclusion.[13]

## Drawing the line: evaluating the nature of the conduct

When determining whether conduct has occurred *in trade or commerce*, the critical question to be asked is whether the conduct *of its nature* bears a trading or commercial character.[14] In arriving at its decision, the Full Court canvassed several cases that were relied upon by Mr Fletcher to support what he contended was the correct characterisation of his conduct. Their Honours' discussion of the cases of *Fasold v Roberts (Fasold)*[15] and *SingTel Optus Pty Limited v Australian Football League (SingTel Optus)*[16] is particularly illustrative of the evaluative process that must be undertaken in order to assess whether the second limb of s 18 is properly called into operation.

In *Fasold*, the court considered whether the delivery of public lectures on the subject of archaeology constituted conduct *in trade or commerce*. Sackville J was alert to the risk of courts being improperly used to stymie legitimate public debate, and to the possibility that the prospect of litigation might deter those with limited resources from engaging in such debate in the first place.[17] Mr Fletcher argued that, like the lecturer in *Fasold*, his conduct was motivated by altruistic rather than commercial interests, and that the blog was primarily used to participate in public discussion and commentary. The Full Court disagreed with that characterisation, however, and held instead that the article was "a promotional activity directed at newspaper franchisees".[18] *Fasold* was therefore of no assistance, and s 18 was clearly applicable.[19]

The decision in *Singtel Optus* was another authority relied upon by Mr Fletcher to remove his case from the reach of s 18. That case concerned comments made by the Chief Executive Officer (CEO) of the Australian Football League (AFL) regarding Optus and its recording of content in respect of which the AFL had copyright. As observed by Mr Fletcher, the fact that the CEO was an industry participant commentating on industry affairs was not determinative of the character of the impugned conduct. Indeed, Edmonds J held that the CEO's comments were "statements of opinion" and "value judgments" that were made *not* in trade or commerce but rather in the context of a "wide-ranging interview" on a wide variety of topics.[20] Mr Fletcher argued that his own conduct was properly characterised the same way. The Full Court, however, distinguished

the two cases on the basis that the *entirety* of Mr Fletcher's article was an attack on a *direct business competitor* for the purpose of *protecting his own business interests*.[21] Thus those collective factors led to an entirely different evaluation of the nature of Mr Fletcher's conduct.

## Conclusion: the practical implications

Courts have long recognised that there is no definitive line separating that which is, and that which is not, conduct occurring *in trade or commerce*. While courts are wary of stifling legitimate discussion or commentary, bloggers should be conscious of the risks of publishing material that is designed to have an impact on trading or commercial activities, whether their own or those of another. The application of the test in *Concrete Constructions* will always necessitate an evaluation of the qualities which might import a trading or commercial character to an activity. If a blog *of its nature* bears a commercial or trading character — as was ultimately decided in Mr Fletcher's case — civil liability pursuant to s 18 can unexpectedly arise.

***Stephanie Hayes***
*Former associate to Senior Member*
*Bernard McCabe*
*Administrative Appeals Tribunal*
*sa.hayes@live.com.au*

## Footnotes

1. *Fletcher v Nextra Australia Pty Ltd* [2015] FCAFC 52; BC201504528.
2. *Concrete Constructions (NSW) Pty Ltd v Nelson* (1990) 169 CLR 594; (1990) 92 ALR 193; [1990] HCA 17; BC9002935.
3. Above n 2, at [7].
4. *Universal Music Australia Pty Ltd v Cooper* (2005) 150 FCR 1; (2005) 65 IPR 409; [2005] FCA 972; BC200505025.
5. Above n 4, at [140].
6. *Nextra Australia Pty Ltd v Fletcher* [2014] FCA 399, at [38].
7. *Village Building Co Ltd v Canberra International Airport Pty Ltd* (2004) 139 FCR 330; (2004) 210 ALR 114; [2004] FCAFC 240; BC200405571.
8. Above n 7, at [59].
9. Above n 6.
10. Above n 1, at [35].
11. Above n 1, at [46].
12. Above n 1, at [47].
13. Above n 1, at [57].
14. See generally B McCabe "Revisiting Concrete Constructions" (1995) 3 *PLJ* 161; B McCabe "Concrete Constructions Turns 15" (2005) 13 *TPLJ* 6.
15. *Fasold v Roberts (Evolution v Creation case/Noah's Ark case)* (1997) 70 FCR 489; 145 ALR 548; (1997) ATPR 41–561; BC9702172.
16. *SingTel Optus Pty Limited v Australian Football League* [2012] FCA 138; BC201200748.
17. Above n 15, at 550.
18. Above n 1, at [54].
19. Above n 1, at [44].
20. Above n 16, at [14].
21. Above n 1, at [56].

# The law of signatures: the signs, they are a changin'

***Peter Moran*** *NORTON GLEDHILL*

## Introduction

The signed contract has been given a special place in the law of contracts. Some have said that a signed contract is the best evidence of both contractual intention[1] and contractual obligations.[2] Such is the importance of a signature that a separate doctrine of mistake has developed especially for signed contracts: namely the plea of *non est factum*.

Despite the importance of the signature in evidencing contracts, the courts have often (and long before the advent of computers) taken a flexible approach by focusing on function over form when determining whether a signature has in fact been applied.[3]

## Electronic signatures in the courts

Jump forward to the internet era and the courts have continued their focus of function over form[4] in upholding signing obligations in an electronic context.

### *Typing a name into an email*

In *J Pereira Fernandes SA v Mehta (Pereira)*,[5] Judge Pelling QC noted that, provided a person inserts their mark into a document with the intention of giving it authenticity, it does not matter if it's a full name; or a first name prefixed by some or all initials; or by using a pseudonym or a combination of letters and numbers. It makes no difference if a person does so in an electronic document or a hard copy.

In this case, the automatic insertion of a person's email address was held to be too incidental to be evidence of the person's intention to give the email authenticity. However, his Honour still held in *obiter dicta* that a person typing his or her name into an email is a sufficient signature for the purposes of satisfying s 4 of the Statue of Frauds (1677) (UK).

While not explicitly referring to Pelling J's *dicta*, the Victoria Supreme Court said essentially the same thing in *Legal Services Board v Forster*[6] where Emerson J held that the requirement for a signature had been met by the insertion of the person's typed named into an email. As distinct from *Pereira*, however, in this case there was no doubt that the person clearly intended this to stand in place of their signature because they said as much in the email itself.

Particularly in the context of the long line of authorities already referred to,[7] the matter would appear to be fairly settled: a person who types their name into an electronic document, including an email, can be held to have signed the document if they intended to authenticate the contract by doing so.

### *Clicking electronic buttons*

The courts in Australia also appear to be quite comfortable in holding that the clicking of some sort of electronic button, by way of accepting contractual terms, is not only sufficient to constitute clear evidence of the acceptance of an offer (and communication of that acceptance)[8] but even to be equivalent to a traditional hard copy signature.[9] Authorities on the issue have existed for several decades and appear to be a relatively settled area of law.[10] This method of acceptance of terms and conditions has been described as a "clickwrap".[11] "Browsewrap", on the other hand, does not involve an explicit acceptance of terms, but simply makes them available for review as part of the contracting process. US decisions on browsewrap agreements indicate that they will be upheld if the user has actual or constructive knowledge of a site's terms and conditions prior to using the site.[12]

A core legal question with such methods of acceptance is in determining at what precise point in the process acceptance actually occurs. Many types of online contracting processes (such as online banking or ticket purchasing systems) offer the counterparty numerous opportunities to withdraw or go back (and the user can always exit their web browser or even sever the internet connection such as by turning their computer off). It is only when the party takes the last definitive step, generally when a person's electronic banking details are processed, and they then lose the ability to withdraw, that they have committed to the transaction and accepted the offer from the vendor. *Cheshire & Fifoot*'s speaks of the emergence of a new contract formation rule for electronic contracts: the "last act" rule whereby the last act is equivalent to acceptance.[13] Determining what is the last act in electronic contracts

could become a much more important issue in determining whether the contract was accepted than whether or not the process used was or wasn't akin to a traditional hard copy "signature".

Also inherent in these processes is that, at some time prior to the click, the person clicking has verified their identity in some way. Without that, the click is of little help as an authentication of a person's intention because the person doing the clicking is not able to be proven. Flowing on from this will no doubt be issues of agency and the extent to which a third party, such as a spouse or a service provider, can bind a party through completing an electronic verification process on their behalf.

### *Other type of electronic verification process*

While contracts exchanged by email and clickwraps/browsewraps currently appear to comprise the most common methods in Australia for authenticating contracts electronically (excluding, perhaps, credit/debit card and online banking transactions), there are a variety of other methods available and which appear likely to become more common in the future. Very few of these methods have been considered by Australian courts.[14]

These methods are, however, starting to make their way into the market place. There are the proprietary signing systems such as DocuSign and EchoSign. There are EDI (electronic data interchange) systems whereby computers communicate and transact with one another directly, sometimes on an automated basis often without human intervention. There are biometric systems and password/hybrid methods and the range of methods used in the banking sector. The question for lawyers and the courts, as regards such a broad spectrum of potential methods, is whether and, if so, how they are to be applied within the existing law of contract.

## What constitutes an electronic signature?

Legislators have attempted to deal with the question of what constitutes a valid signature in an electronic context by defining its required attributes. Interestingly, in doing so, they have often gone beyond the attributes required for paper based signatures. For example, Smedinghoff and Bro[15] refer to legislation introduced in California in the mid-90's which required that an electronic signature was only legally effective as a signature if it was:

- unique to the person using it;
- capable of verification;
- under the sole control of the person using it; and
- linked to the data in such a manner that if the data is changed, the signature is invalidated.

It is a rare occurrence to verify either a signature or the precise terms of a paper contract at the time of execution and neither render the signature legally ineffective at the time. Instead, these issues are left as evidentiary problems if the contract has to be enforced.

Our own Electronic Transaction Act regimes have taken a slightly simpler approach. An electronic signature is satisfactory provided:[16]

- A method is used to both identify the person signing and indicate their intention.
- The method is as reliable as is appropriate.
- The counterparty consents to the method used.

This follows the approach suggested by the UN in the UNCITRAL Model Law.[17] Other jurisdictions have taken similar but slightly different approaches: for example, the US regimes generally require an electronic process logically associated with a record that is adopted by a person with the intent to sign that record.[18]

Common across these regimes would appear to be the following attributes:

- The signatures must identify and authenticate a legal person (ie, is the signature genuinely from the person asserting to have provided it?).
- It must indicate their approval (ie, did they intend to approve the contract terms by providing the signature?).
- Is the link between the signature and the contract of sufficient integrity (ie, is it clear that the document exchanged with the offer or the same as that signed by the accepting party?).

The presence of these three attributes then generally ensure the satisfaction of a number of essential elements of a contract:

- offer;
- acceptance;
- intention to be legally bound; and
- certainty of contractual terms.

When applied against these common attributes, an email scan of a full contract meets the second and third but not the first (unless the scan of the signature is separately verified). An email scan of just the signing page only meets the second attribute. Despite this email scans of hard copy signed contracts appear to be the most common form of electronic contract being used by Australian lawyers currently. This evidenced by the joint protocol produced recently by a number of leading Australian law firms regarding "remote signing" of contracts.[19] Remote signing, in this case, was given the very limited definition of "the exchange of scanned documents or signature pages by email". The protocols chose to explicitly ignore "the effectiveness of proprietary online products for the electronic creation, execution and storage of documents, such as DocuSign". This

is presumably because such products are not being used in the vast majority of electronic contracts facilitated by these firms.

## The evolution of electronic authentication methods

Whether lawyers are comfortable with them or not, the market will ultimately be the driver of different authentication methods by which to confirm a customer's identity and their agreement to their terms and conditions. In such circumstances, the job of lawyers will in some ways become easier in advising on contract disputes. Contract fraud should become harder to commit. Determining the "who, where and when" of a contract and its formation should be a mere matter of reviewing the metadata contained within the contract itself. The parties' intentions should be much clearer. The integrity of the document will be linked to the integrity of the electronic system and could therefore be the system provider's problem more than the party seeking to enforce the contract.

Instead, new issues may start to consume the courts' time. Proving (or even establishing) the identity of an online persona/avatar may become a more common problem in enforcing a contract. Determining the appropriate jurisdiction and location at which the contract is formed when both parties are "in the cloud" will continue to confound parties seeking to enforce contractual rights. Ensuring that metadata has not been tampered with and/or using technological experts to verify the integrity of the electronic contracting system may become more important evidentiary issues.

## Tips for practitioners

In advising upon the use of electronic signatures in contracts, practitioners should make sure to:

- focus on function over form (ie, a signature is not a "thing" but a process, used to evidence the objective intention of the contracting parties)[20];
- not forget that a signature assists with evidencing core contract law principles:
  - — offer;
  - — acceptance;
  - — intention to be legally bound; and
  - — certainty of terms.
- ensure the identity of a person providing an electronic signature is clear and authentic;
- ensure that the intention of the parties providing the signature is clear and that the parties have consented to the signing method; and
- ensure the contractual terms are linked with the electronic signature and unable to be tampered with.

***Peter Moran***
*Principal*
*Norton Gledhill*
*Peter.Moran@norgled.com.au*

## Footnotes

1. *L'Estrange v Graucob* [1934] All ER Rep 16; [1934] 2 KB 394; (1934) 103 LJKB 730; 152 LT 164 and *Life Insurance Co of Australia Ltd v Phillips* [1925] VLR 311; (1925) 36 CLR 60; 31 ALR 206; BC2500039.
2. N Seddon, R Bigwood & M Ellinghaus *Cheshire & Fifoot's Law of Contract* (10th edn) LexisNexis, Australia 2012, p 735.
3. See, for example, *Baker v Dening* (1838) 8 A&E 94; *Redding's (otherwise Higgins') Goods, Re* (1850) 14 Jur 1052; 2 Rob. Ecc. 339; *Morton v Copeland* (1855) 16 CB 517; *Caton v Caton* (1867) LR 2 HL 127; *Howley v Whipple,* 48 N.H. 487 (1869); *Brydges v Dix* (1891) 7 TLR 215; *France v Dutton* [1891] 2 Q.B. 208; *Evans v Hoare* [1892] 1 QB 593; *Hill v Hill* [1947] Ch 231; *Goodman v J Eban* [1954] 1 QB 550; [1954] 1 All ER 763; [1954] 2 WLR 581; *London County Council v Agricultural Food Products Ltd sub nom London County Council v Vitamins Ltd (All ER)* (1955) 53 LGR 350; [1955] 2 QB 218; (1955) 165 EG 444; [1955] 2 WLR 925; *Lazarus Estates, Ltd v Beasley* [1956] 1 QB 702; [1956] 1 All ER 341; *Cook (decd), In the Estate of* [1960] 1 All ER 689; (1960) 104 Sol Jo 311; [1960] 1 WLR 353.
4. Although there are occasions where judges have expressed more conservative views, such as the dissenting judgement of Denning LJ in *Goodman v J Eban* where he was not convinced that the application of a facsimile signature using a rubber stamp constituted a signature because it carried no guarantee that it was affixed by the person claiming to have signed it.
5. *J Pereira Fernandes SA v Mehta* [2005] All ER (D) 264 (Apr); [2006] 2 All ER 891; [2006] 1 WLR 1543; [2006] 1 All ER (Comm) 885.
6. *Legal Services Board v Forster* [2010] VSC 192; BC201002933.
7. That is, the authorities listed in n 3 above.
8. Clicking on "send this order" and "purchase ticket" buttons on an online form (after having provided identification) have been held to constitute the signing of an electronic contract: *eBay International AG v Creative Writing Festival Entertainment Pty Ltd* (2006) 170 FCR 450; (2006) Aust Contract R 90–248; [2006] FCA 1768; BC200610545. See also *Hospitality Group Pty Ltd v Australian Rugby Union Ltd* (2001) 110 FCR 157; (2001) ATPR 41–831; [2001] FCA 1040; BC200104902.
9. The transmission of an electronic application which states: "I agree by transmitting [this submission] electronically … it has the same status as if I had signed it" was held to be equivalent to a signature: *Harding v Brisbane City Council* [2009] 197 QPELR 207.
10. The US Supreme Court formed a fairly definitive view on the matter, albeit in the context of software licences, as long ago as 1996: see *ProCD Inc v Zeidenberg* (1996) F 3d 1447. See also

*US v Drew* 259 FRD 449 and B Fitzgerald, A Fitzgerald, G Middleton, E Clark and YF Lim *Internet and E-Commerce Law, Business and Policy* Thomson Reuters, Australia 2011 pp 763 and 765 where they note that on every occasion that clickwrap agreements have been considered by courts in the United States, they have been found to be enforceable.

11. Clickwrap agreement was an adaption, in an internet environment, of the term "shrinkwrap" which was used in the context (eg, the ProCD case) of software licences deemed to be entered into at the point of removing the shrinkwrap from the software packaging.
12. *Internet and E-Commerce Law, Business and Policy*, above n 10, at p 765.
13. Above n 2, at p 147.
14. *Getup Ltd v Electoral Commissioner* (2010) 189 FCR 165; (2010) 268 ALR 797; [2010] FCA 869; BC201005838 is one such case where applying an ordinary signature via a digital pen on a tablet was held to be a valid signature.
15. T Smedinghoff and R Hill Bro "Moving with Change: Electronic signature legislation as a vehicle for advancing e-commerce" (1999) 17 *John Marshall Journal for Computer and Information Law* 723.
16. Electronic Transactions Act 1999 (Cth), s 10.
17. United Nations Commission on International Trade (UNCITRAL) *The Model Law on Electronic Commerce* (1996).
18. The US has numerous pieces of legislation dealing with electronic signatures such as s 206 of the Electronic Signatures in Global and National Commerce Act, s 1710 of the Government Paperwork Elimination Act and s 2 of the Uniform Electronic Transactions Act. See also the European Union Directive on Community Framework for Electronic Signatures 1999.
19. The Walrus Committee *Remote signing protocols for financing transactions* — (2015) 43 *ABLR* 497.
20. YF Lim, *Cyberspace Law* (2nd edn) Oxford University Press 2008 p 93; C Reed "What is a Signature" (2000) 3 *The Journal of Information, Law and Technology*.

# The "Netflix" tax

***Geoffrey Mann**, **Shilpa Jain** and **Jadie Teoh** ASHURST*

## Practical tips for lawyers

- When giving advice to non-resident suppliers making supplies into Australia, consider whether "reasonable steps" have been taken to determine if the supply is being made to an "Australian consumer".
- Consider, if required, whether to register the supplier as a full registration or a limited registration entity.

## Introduction

In the Federal Budget released in May 2015, the Commonwealth Government proposed imposition of goods and services tax (GST) at 10% on supplies of intangibles to Australian consumers (Netflix tax) by non-resident suppliers. The government released an exposure draft of the legislation in May 2015 and a second exposure draft, the Tax Laws Amendment (GST Treatment of Cross-Border Transactions) Exposure Draft Bill 2015 (Cth) (Second Exposure Draft) in October 2015.[1] It is intended that the amendments to the GST legislation will take effect from 1 July 2017.

The amendments are consistent with reforms in a number of other countries including Norway, Japan and New Zealand (discussed below) to extend the scope of their value added taxes to the growing area of cross-border supplies of intangibles to consumers in those countries.

The implementation of the Netflix tax is intended to ensure that the GST revenue base does not steadily erode over time through the increasing use of foreign digital supplies by Australian consumers and that local suppliers are not at a tax disadvantage relative to overseas suppliers.

## Summary of current law

Under the current GST law, GST is payable on taxable supplies and taxable importations.

A taxable importation is an importation of goods that are entered into Australia for consumption within Australia, provided the importation is not specified to be a non-taxable importation.

Generally, for a supply to be a taxable supply it must, among other things, be connected with the Australian "indirect tax zone" (ie, supplies made or done in Australia or goods delivered within Australia).

The current GST law also ensures that entities that are registered or required to be registered for GST are in the same net GST position in respect of intangibles acquired for their Australian activities from overseas as they are for things acquired locally by requiring the recipient of the supply (and not the supplier) to pay GST. This is known as the "reverse charge" rule. However, this rule does not extend to entities that are not registered or required to be registered for GST (ie, consumers).

The issue that was identified by the Australian Government with the operation of these rules was that the importation of services or intangible property by consumers would never be a taxable importation (as taxable importations were limited to goods) and will often also not be a taxable supply under the current "connected" rules. Further, as mentioned above, they would also not be subject to the "reverse charge" rule.

## The Netflix tax

The Second Exposure Draft provides that all "inbound intangible consumer supplies" made to "Australian consumers" will be considered to be "connected" with Australia, and subject to GST, regardless of whether the supplier is an Australian resident or non-resident. Consistent with the general rules, the suppliers of such supplies will be required to register for GST if the total of their GST turnover for a financial year meets or exceeds the GST turnover threshold of $75,000 ($150,000 for non-profit entities). Under the provisions, suppliers that make at least one inbound intangible consumer supply may also elect to be a limited registration entity. They may later revoke this election to become a full registration entity.

The Netflix tax will result in supplies of digital products, such as streaming or downloading of movies, music, apps, games and e-books, as well as other services, such as consultancy, advisory services and brokering, receiving equivalent GST treatment whether they are supplied by a local supplier or a foreign supplier.

A supply is an "inbound intangible consumer supply" if it is a supply of anything other than goods or real property that is not done wholly in the indirect tax zone or the supply is made through an enterprise the supplier carries on in the indirect tax zone. The Second Exposure Draft allows for inbound intangible consumer supplies

to be GST-free or input taxed where the Treasurer determines so for a specified class of supplies.

An "Australian consumer" is an Australian resident (other than an entity that is an Australian resident solely because the definition of Australia in the Income Tax Assessment Act 1997 includes the external Territories) that:

(a) is not registered for GST; or
(b) if the entity is registered for GST — the entity does not acquire the supply to any extent for the purpose of an enterprise that the entity carries on.

Under the amendments, if a supplier that would otherwise be liable for GST in relation to supplies of services and intangibles takes reasonable steps to obtain information concerning whether the recipient of the supply is an Australian consumer and based on the information reasonably believes that the recipient is not an Australian consumer, then the supplier may treat the supply as if it has been made to an entity that was not an Australian consumer (and not subject to GST), even if this is later found to not have been the case. What constitutes "reasonable steps" depends on the context of the particular supply.

The amendments also make changes to the rules for ascertaining an enterprise's GST turnover, which in turn determines whether registration for GST is required. Usually, an entity's GST turnover includes, among other things, the value of the GST-free supplies the entity makes that are connected with the indirect tax zone. However, this would mean that the making of a significant number of supplies by overseas suppliers to Australian residents which would, under these rules, be connected with the indirect tax zone, but which are used and enjoyed outside the indirect tax zone and therefore GST-free, would require GST registration of the suppliers. An example of this would be an Australian getting a haircut in Germany. Thus, the amendments exclude GST-free supplies from GST turnover. The amendments also modify the exclusion for supplies of rights so that a supply of a right or option to an Australian consumer will be included in the GST turnover of the supplier entity if the underlying supply is not a supply of goods or real property and the supply is not GST-free.

### *Electronic distribution platform (s 84–65)*

In some circumstances, the GST liability is shifted from the supplier to the operator of an "electronic distribution platform" through which the supplies of inbound intangible consumer supplies are made. This will occur if the operator of the electronic distribution platform controls any of the key elements of the supply such as authorising billing, setting the terms and conditions of the supply or authorising the delivery arrangements.

A service is an "electronic distribution platform" if the service allows entities to make supplies available to end-users, the service is delivered by means of electronic communication and the supplies are to be made through electronic communication.

If supplies are made through multiple electronic platforms, only the first operator to authorise a charge or receive any of the consideration for the supply will be treated as making the supply. If none of the operators meet this requirement, it is the first operator to authorise the delivery of the supply that will be liable. The Commissioner may also, by legislative instrument, prescribe additional rules to override or supplement these general rules (s 84–55).

#### *Limited registration*

Entities may choose to be limited registration entities. A limited registration entity will only have to provide minimal information to the Commissioner and have more simplified administrative arrangements under the amendments, for example, such entities must have a quarterly tax period and may not elect to pay GST by instalments. Limited registration entities are also not entitled to input tax credits.*(*Sch 1 Pt 1 subdiv 84-D*)*

The amendments also allow for a limited registration entity to become a full registration entity effective back to the start of the preceding financial year. In such circumstances, the entity will be able to claim input tax credits over the full amount of this period in which they were registered for GST. We recommend that limited registration entities keep tax invoices and maintain other records so as to be able to claim input tax credits should they at a later time elect to become a full registration entity.

## Transitional provisions

Periodic or progressive supplies will be treated as separate supplies in each tax period and the proportion of such supplies made after 1 July 2017 will be subject to the changes. Supplies made under an agreement entered into before 7.30 pm on 12 May 2015 will not be affected by the transitional rules except to the extent it relates to tax periods occurring on or after 1 July 2019. (Sch 1 Pt 3 s 34)

***Geoffrey Mann***
*Partner*
*Ashurst, Melbourne*
*geoffrey.mann@ashurst.com*

***Jadie Teoh***
*Senior Associate*
*Ashurst, Melbourne*
*jadie.teoh@ashurst.com*

***Shilpa Jain***
*Lawyer*
*Ashurst, Melbourne*
*shilpa.jain@ashurst.com*

## Footnotes

1. Found at www.treasury.gov.au.

# The URS — 2 years on

***Marie Wong*** *and* ***Bindhu Holavanahalli*** *WRAYS*

## Tips for IP practitioners

- URS should only be utilised in clear-cut cases where the trade mark holder has registered rights in a distinctive trade mark, and the domain name holder is clearly acting in bad faith.
- The complainant must be the registered proprietor of the relevant trade mark.
- UDRP should be preferred where the complainant wants the domain name transferred or cancelled (as opposed to suspended), where the trade mark is slightly generic or descriptive, or where the complainant is not clearly acting in bad faith.

The Uniform Rapid Suspension System (URS) is an administrative proceeding intended to complement the Uniform Domain-Name Dispute Resolution Policy (UDRP). The first URS decision was issued on 29 October 2013.[1]

The URS is governed by the URS Procedure,[2] which sets out the URS claims process, and the URS Rules,[3] which have been prepared to help service providers (URS Providers) implement URS in a consistent manner. To date, only three URS Providers have been appointed.[4]

## URS v UDRP claims

A complainant can only bring a URS proceeding in respect of a dispute over a domain name that incorporates a generic top-level domain (gTLD) that was introduced after 1 January 2013.[5] Disputes in respect of domain names with older gTLDs (eg, .com or .net domains) can only be dealt with under the UDRP.

The URS was touted as a cheaper and quicker alternative to the UDRP, to be used in clear-cut cases of cybersquatting. The filing fee for a URS complaint is typically US$500, whereas the filing fee for a UDRP is approximately US$1500.[6] URS proceedings are also typically determined within 3 weeks, whereas UDRP determinations are not usually issued before 6 weeks from the filing date.

Despite being both cheaper and quicker, the URS suffers from the following disadvantages which may make the UDRP more attractive to potential complainants in some circumstances:

- Though both the URS and the UDRP are assessed against the same basic elements (namely, that the domain name is identical to the complainant's trade mark, the respondent does not have any rights or legitimate interests in the domain name, and that the domain name was registered in bad faith), the complainant is held to a higher standard of proof in a URS proceeding. The complainant in a URS proceeding must present clear and convincing evidence of each of the three elements, and also show that there is no genuine contestable issue. In contrast, the complainant in a UDRP proceeding need only establish their case on the balance of probabilities.
- The only remedy available to a successful complainant under the URS is suspension of the domain name until the end of the registration term (at which point the domain can be purchased by any party). In contrast, under the UDRP, a complainant can obtain a transfer or cancellation of the disputed domain name.
- The complainant must have a registered trade mark and cannot rely on common law trade mark rights.
- The gTLD of the disputed domain name must have been introduced after 1 January 2013 (therefore excluding.com or.net domains).
- A URS complaint is limited to 500 words (within which the complainant must present clear and convincing evidence for all three elements), whereas the UDRP proceedings allow complaints of up to 5000 words.

In cases that have been decided under the URS, complainants have failed on a number of grounds where they may have succeeded under a UDRP proceeding (with the benefit of providing additional evidence in a longer complaint, or where the burden of proof is lower) such as:

- failure to establish that the complainant is the owner of the registered trade mark where the complaint was filed in the name of one entity but the trade mark was registered in the name of a separate, related entity;
- failure to establish that the respondent was acting in bad faith because the complainant's registered trade mark was not particularly distinctive;

- an apparent requirement to prove that the trade mark in question is "strong" in order to draw inferences to establish the second and third elements; and
- failure to demonstrate that the respondent had a pattern of recidivist behaviour.

For example, in *Aeropostale Procurement Company, Inc v Michael Kinsey*,[7] the complaint was denied because the trade marks were registered in the name of related companies R H Macy & Co, Inc, Aeropostale West, Inc, and Aeropostale, Inc, but the complaint was brought in the name of Aeropostale Procurement Company, Inc. The decision maker suggested that if the complainant had shown evidence of a relationship between the trade mark owners and the complainant (within the 500 word complaint), it may have been successful.

In *Virgin Enterprises Ltd v lawrence fain*,[8] Virgin Enterprises Ltd sought to suspend the registration of the domain name branson.guru. Despite advancing evidence of trade mark registrations for the word "BRANSON" in South Africa, the complaint was denied. The examiner considered that the complainant did not advance enough evidence to show that it has a significant reputation in the term BRANSON, which was relevant to both the second and third elements of the URS procedure.

Further, it was noted that the disputed domain was being used as a generic, monetized parking page without actual reference to the complainant's trade mark, or to Richard Branson. Accordingly, the examiner decided that the lack of a strong trade mark meant that he could not then draw inferences about whether the domain was registered or used in bad faith, especially when the respondent had not used the domain to make any references to the complainant or Richard Branson.

In contrast, Virgin Enterprises was successful in *Virgin Enterprises v kimerly kerg*,[9] concerning the domain name virgingalactic.guru. The complainant advanced evidence of a trade mark registration for VIRGIN GALACTIC in Europe. Though the domain name merely resolved to a click through site, the examiner found that the second and third elements were established because the domain name was identical to the trade mark, the complainant had not provided any authorisation for the respondent to use the trade mark and because the domain name was registered and was being used in bad faith to attract users for commercial gain.

It appears that the difference in result between the VIRGIN GALACTIC decision and the BRANSON decision is contingent on the "strength" of the trade mark rather than the use that is being made of the domain name by the respondent.

In *RMIT University v Byron Ventures Pty Ltd*,[10] which concerned the domain name rmit.education, the complaint was denied on the basis that the complainant failed to submit any evidence as to the second and third elements of the URS. This was despite the fact that the respondent did not provide a response to the complaint, and that RMIT is a well-known educational institution in Australia.

The *Prudential Insurance Company of America v Terrance McQuilkin et al*,[11] concerned the domain name www.rocksolid.finance, where the complainant had a registration for "ROCK SOLID" and operated in the financial services field. The complainant failed because "ROCK SOLID" was considered to be descriptive, and also because the complainant had not advanced sufficient evidence of the respondent's bad faith such as a bad faith attempt to profit from the goodwill of the complainant.

It can be seen from the examples above that the URS is most appropriate in a clear-cut case of infringement of a trade mark with sufficient notoriety, where the complainant is concerned to stop an instance of cybersquatting, but where the complainant does not wish to actually acquire the domain name.

The URS may not be appropriate if the trade mark on which the complainant relies is slightly generic or descriptive, in which case persuasive arguments or substantial evidence is likely to be required to convince the examiner of the respondent's bad faith (which cannot properly be achieved within the 500 word limit for URS complaints), even in the absence of any response from the respondent.

## How has the URS been received?

It has now been nearly 2 years since the first URS determination was made (in respect of www.facebok.pw, which was decided in favour of the complainant).

As at 15 October 2015, there have been 387 URS cases filed with the National Arbitration Forum (the Forum) and 28 cases determined at the Asian Domain Name Dispute Resolution Centre, which are at this stage the only approved URS providers.

Over the same period, approximately 5000 UDRP proceedings have been filed with WIPO. Obviously, one would expect the number of URS cases filed to be significantly lower than the number of UDRP filings as the URS is only available in respect of new gTLDs introduced after 1 January 2013, whereas the UDRP is open to all gTLDs.

However, the question remains as to whether complainants have embraced the new URS system where both the URS and UDRP have been available, or whether the disadvantages of the URS procedure has meant that complainants have opted for the UDRP

proceedings in preference, despite the cost savings and efficiency offered by the URS.

There have been approximately 750 new gTLDs introduced since 1 January 2013. Though it is beyond the scope of this article to evaluate all of these new gTLDs, we have compared the number of UDRP complaints versus the number of URS complaints filed in respect of some of the most popular new gTLDs. The results of our survey are summarised in the table below.

| gTLD | Number of UDRP complaints | Number of URS complaints |
|---|---|---|
| .link | 4 | 9 |
| .holdings | 5 | 5 |
| .company | 16 | 6 |
| .careers | 5 | 5 |
| .technology | 4 | 5 |
| .club | 34 | 31 |
| .ventures | 3 | 7 |
| .clothing | 12 | 6 |
| .trade | 5 | 0 |
| .nyc | 4 | 5 |
| .london | 6 | 6 |
| .website | 12 | 8 |
| .services | 5 | 4 |
| .xyz | 45 | 25 |
| .top | 11 | 27 |
| **Total** | **171** | **149** |

Though it is not possible to make any generalised statements due to the small sample size, it appears that complainants are opting to use both the URS and UDRP in roughly equal proportions.

It also appears that the URS is being utilised appropriately by complainants with strong clear-cut cases. Of the 330 finalised URS complaints filed with the Forum, the complainant has succeeded in 315 cases — that is, a success rate of approximately 95%. Under the UDRP, the percentage of successful complainants is approximately 90%.[12]

Therefore, despite the higher burden of proof for complainants, the URS appears to be being utilised by applicants who are able to satisfy this elevated burden of proof. A review of some URS decisions, however, indicates that the standard of proof may be inconsistently applied between cases, and also, that in some cases, detailed reasons are not being provided for the determinations.

A review of the complainants in UDRP cases versus those for URS cases, since 29 October 2013, reveals that although some complainants appear to be filing complaints in both forums (such as Alibaba Holdings Group, which has filed 23 URS cases and 12 UDRP cases in respect of ccTLDS not covered by the URS), some complainants appear to prefer the URS. For example, over the same period since 29 October 2013:

- Bloomberg LP, which has filed nine URS cases, has filed zero UDRP cases; and
- Deutsche Lufthansa AG has filed 32 URS cases and zero UDRP cases.

Under the URS Procedure document, a review of the URS procedure was to be initiated 1 year after the first URS determination was handed down, that is, on 29 October 2014. Upon completion of the review, a report was to be published regarding the usage of the procedure, including statistical information. The report was then to be open for public comment on the usefulness of the procedure. This document, when published, will provide a more comprehensive overview of the effectiveness and uptake of the URS procedure, although we are yet to see any documentation, nearly a year on from when the review was to be initiated.

Nevertheless, based on our review, the URS seem to be an appropriate (cheaper and quicker) alternative to the UDRP in cases of cybersquatting relating to strongly distinctive and well-known trade marks.

***Marie Wong***
*Principal*
*Wrays*
*Marie.Wong@wrays.com.au*

***Bindhu Holavanahalli***
*Lawyer*
*Wrays*
*Bindhu.Holavanahali@wrays.com.au*

**About the authors**

*Marie is an intellectual property lawyer and registered trade marks attorney. Marie is a Principal at Wrays, where she heads up the trade marks, media and technology team. Marie has diverse experience in trade mark law, commercial agreements and consumer law, and has been involved in numerous domain name disputes, including the filing of UDRP complaints.*

*Bindhu is an intellectual property lawyer at Wrays. Bindhu has experience in trade mark law, consumer law and patent law. She has also been involved in a number of domain name disputes, and has experience in filing UDRP complaints.*

## Footnotes

1. *Facebook Inc v Radoslav* FA1308001515825. The complainant, Facebook Inc, was successful in suspending the domain

www.facebok.pw. Facebook demonstrated that the respondent had engaged in a pattern of illegitimate domain name registrations, and thus that the disputed domain name had been registered and used in bad faith.

2. ICANN, *Official URS Procedure*, 1 March 2013, www.newgtlds.icann.org.
3. ICANN, *URS Rules Updated*, 28 June 2013, www.newgtlds.icann.org.
4. The National Arbitration Forum was confirmed as a URS provider on 21 February 2013 (ICANN, *ICANN Appoints First URS Provider*, www.newgtlds.icann.org) and the Asian Domain Name Dispute Resolution Centre was confirmed as the second URS provider on 19 April 2013 (ICANN, *ICANN appoints Additional URS Provider*, www.newgtlds.icann.org). MFSD Srl (MFSD) was confirmed as the third URS provider on 15 December 2015.
5. Above n 3, definition of "New gTLD".
6. For one domain name (for a UDRP panel consisting of one member).
7. Claim Number: FA1403001550933.
8. Claim Number: FA1402001545807.
9. Claim Number: FA1402001545806.
10. Claim Number: FA1407001571371.
11. *Prudential Insurance Company of America v Terrance McQuilkin* et al 2:2015cv01276.
12. Calculated on the basis of WIPO statistics from complaint outcomes in 2014 and 2015.

**For editorial enquiries and unsolicited article proposals please contact Katharine Chia at katharine.chia@lexisnexis.com.au.**
**Cite this issue as (2016) 19(2) *INTLB***
**SUBSCRIPTION INCLUDES: 10 issues per volume plus binder www.lexisnexis.com.au**
**SYDNEY OFFICE: Locked Bag 2222, Chatswood Delivery Centre NSW 2067**
**CUSTOMER RELATIONS: 1800 772 772**
**GENERAL ENQUIRIES: (02) 9422 2222**
**ISSN 1329-9735 Print Post Approved PP 244371/00049**