Ashurst Australia
26 August 2013

ashurst

IT, Communications & Media Update

In this update

Editorial

Welcome to this edition of the ICM update.

This update contains some interesting articles, including:

- an article about whether step in rights in IT contracts may be a security interest;
- an article about the Defence White Paper on cyber security; and
- an article considering the implications of some Australian courts' findings that the "average internet user" is viewed as technologically advanced.

We also include the following case notes:

- *SF v Shoalhaven City Council* [2013] NSWADT 94 regarding privacy and CCTV camera footage;
- *Telstra Corporation Limited v Indigo SC* [2013] VCAT 659 (1 May 2013) regarding Telstra's quest for quality of service in rural areas; and
- *ACCC v Excite Mobile Pty Ltd* [2013] FCA 350 regarding the ACCC's approach to telecommunications services providers use of telemarketers.

I hope you enjoy reading this material.

Susan Goodman
Senior Associate
Sydney
T: +61 2 9258 6497
E: susan.goodman@ashurst.com

Step-in rights in IT contracts may be a security interest

WHAT YOU NEED TO KNOW

- A recent New Zealand case has confirmed that construction contract step-in rights can constitute a security interest under the New Zealand *Personal Property Securities Act 1999* (NZ) (NZ PPSA). A similar conclusion is likely to follow under the Australian *Personal Property Securities Act 2009* (Cth) (PPSA).
- This means that depending on their terms, technology outsourcing contract step-in rights may create security interests under the PPSA as well, in which case they will only be effective if they have been properly perfected. Even if a principal does perfect its step-in rights, it may not be able to exercise those rights effectively if the contractor has granted security to someone else.

WHAT YOU NEED TO DO

- Principals should treat step-in rights which give rise to an interest in a contractor's property as a security interest under the PPSA, and perfect them by registration on the Personal Property Securities Register.
- Principals should register their interests at the time the contract is entered into, and not wait until they actually need to step in.
- Even if it is not clear that a step-in right gives rises to a security interest, principals should consider registering the right in any event to best achieve protection.

A recent decision of the High Court of New Zealand, *McCloy v Manukau Institute of Technology* [2013] NZHC 936, concerned a dispute between the receivers of a construction supplier (Mainzeal) and a customer of Mainzeal (Hobson Gardens) regarding equipment that Mainzeal had been using to complete some construction works for Hobson Gardens on Hobson Gardens' property.

The construction contract between Mainzeal and Hobson Gardens was based on the standard New Zealand Institute of Architects' contract terms. It provided that if Mainzeal went into receivership and the receiver did not take over the construction work, Hobson Gardens could terminate the contract. The contract said, if Hobson Gardens so terminated the contract, that Hobson Gardens would be deemed to be in possession of the contract works, and that Mainzeal's interest in the equipment would be transferred to Hobson Gardens. Hobson Gardens would then be entitled to use the equipment to complete the works, and to sell Mainzeal's interest in the equipment and use the sale proceeds to pay money that Mainzeal owed to it.

Mainzeal went into receivership and its receiver, appointed by the Bank of New Zealand (BNZ), declined to take over the construction works. Hobson Gardens then terminated the contract and asserted that it was now in possession of the works. The receiver claimed that it was entitled to the equipment under BNZ's securities. Hobson Gardens resisted this.

Were the step-in rights a security interest?

The receivers argued that Hobson Gardens' step-in rights were a security interest for the purposes of the NZ PPSA, and that BNZ's security interest had priority. Hobson Gardens argued that its step-in rights were not a security interest, so that the priority rules in the NZ PPSA did not apply.

The Court held that the purpose and wording of the step-in rights amounted to an in-substance security interest: a "transaction that in substance secured payment or performance of an obligation". This conclusion was supported by the following indicators:

- the step-in clause was clearly intended to give Hobson Gardens a form of security over Mainzeal's interest in the equipment; and
- the step-in rights were designed to enable Hobson Gardens to complete the contract works and sell the equipment to cover any liability of Mainzeal to Hobson Gardens resulting from Mainzeal's failure to complete the works.

Whose security interest had priority?

Where there are two competing security interests, the NZ PPSA provides that a perfected security interest prevails over an unperfected security interest. BNZ had perfected its security interest by registration, but Hobson Gardens had not, so BNZ's security interest prevailed over Hobson Gardens'.

It is worth noting that Hobson Gardens did not perfect its security interest over the equipment by possession, even though it had taken possession. While it is possible under the NZ PPSA to perfect a security interest by taking possession of the collateral, possession will not perfect a security interest if the possession results from seizure or repossession (section 41(b)(ii) of the NZ PPSA). This meant that taking possession as part of exercising its step-in rights did not serve to perfect Hobson Gardens' security interest as well.

Implications for outsourcing contracts in Australia

Technology outsourcing contracts will typically contain a step-in clause. Under this clause, where a specified trigger event occurs (often where the contractor has materially breached its obligations or is likely to do so), the principal under the outsourcing contract may "step in" to take back responsibility for the services provided by the contractor. There is no standard form of step-in clause for a services contract, and the clause can take a variety of forms, such as:

- a bare contractual right to access the contractor's systems to conduct the operations;
- a contractual right to access and modify the contractor's systems, including a right to modify source code;
- transfer of title to the contractor's systems to enable the principal to conduct operations, with a right to sell to cover costs; and
- a contractual right to access the contractor's systems, and to hold a lien over the systems until all of the principal's costs are recovered.

Even before the *McCloy* decision, many Australian practitioners were of the view that certain types of step-in rights (such as those in *McCloy*) were likely to give rise to a security interest under the PPSA. The decision in *McCloy* has confirmed that view.

Whether a particular step-in clause gives rise to a security interest will turn in particular on whether the clause gives the principal an interest in the contractor's property. On this basis, the first two examples listed above are unlikely to be security interests (as they give the principal only bare contractual rights). The third and fourth examples, however, are likely to be security interests, and will need to be properly perfected if the principal wants to be able to rely on them.

Consequences for Australian principals

If a principal's step-in rights do give rise to a security interest, then the step-in rights are at risk of being of little practical value if they are not perfected. Similar to New Zealand, the only option open to principals to perfect the security interest is by registration on the Personal Property Securities Register. The PPSA does also allow a secured party to perfect its security interest by taking possession, but like the NZ PPSA, the PPSA provides that possession will not perfect a security interest if it results from seizure or repossession (section 21(2)(b) of the PPSA).

If a principal does not protect the security interest under its step-in rights by registration as early as possible, it exposes itself to a number of risks:

- if the security interest is not perfected, the principal's rights under the step-in clause to use and then sell the materials and equipment will be ineffective upon the insolvency of the contractor (section 267 of the PPSA);
- if the security interest is not perfected within 20 business days of the contract coming into force and the contractor is an Australian company, the principal's rights will be ineffective, even if the security interest is perfected outside that timeframe, if the contractor becomes insolvent within six months after it is so perfected (section 588FL of the *Corporations Act 2001*); and
- even if the contractor is not insolvent, the principal's rights under the step-in clause to use and then sell the materials and equipment will be defeated by any perfected security interests over them (section 55(3) of the PPSA).

Even if the principal does perfect its security interest as soon as possible, it needs to be aware that its rights under the step-in clause to use and then sell the materials and equipment will be defeated by any other perfected security interest that has an earlier priority time (section 55(4) of the PPSA).

What you need to do

The *McCloy* decision suggests that a principal under an IT services contract with step-in rights should proceed on the basis that the step-in rights are a security interest for the purposes of the PPSA, if the step-in rights give it an interest in the contractor's property.

If the step-in rights are a security interest

- If the step-in rights do give rise to a security interest, the principal should perfect its security interest by registration as early as possible, and in any event within 20 business days of signing the contract.
- The principal might also want to search the Personal Property Securities Register before signing the contract, to see whether any other secured parties have a security interest that could defeat the principal's ability to use its step-in rights.
- If there are, the principal should consider requiring the contractor to persuade those other secured parties to agree that the principal's interest will take priority over them, despite the fact that they are registered first. This may or may not be commercially practicable.

If the step-in rights might be a security interest

- If it is not clear that a step-in clause gives rise to a security interest, it may be nonetheless prudent for a principal to register a financing statement on the Personal Property Securities Register, in case a court later holds that it is a security interest.
- If a principal is considering this, however, it needs to be mindful of section 151(1) of the PPSA, which provides that a person is subject to a civil penalty for breach of the PPSA if they apply to register a financing statement but do not believe on reasonable grounds that they have (or will have) a security interest.

Contacts

Tim Brookes
Partner
Sydney
T: +61 2 9258 5770
E: tim.brookes@ashurst.com

Bruce Whittaker
Partner
Melbourne
T: +61 3 9679 3212
E: bruce.whittaker@ashurst.com

Tanvi Mehta
Lawyer
Sydney
T: +61 2 9258 6372
E: tanvi.mehta@ashurst.com

Cyber security emphasised as priority in Defence White Paper

WHAT YOU NEED TO KNOW

- The Defence White Paper demonstrates the importance the Government is placing on managing the risks posed by cyber threats. The Government recognises the benefits of having the upper hand when it comes to cyber security and is seeking collaboration with the private sector to help strengthen Australia's defensive and offensive capabilities.
- The White Paper describes the role of the private sector in the Government's development of cyber capabilities as a partnership, but does not specify how this partnership will operate.
- Cyber security is not restricted to a warfare priority in the White Paper, but is described as a capacity that is also critical in peacetime to protect and build confidence in national security, economic prosperity and social wellbeing.

In a world where globalisation and new technologies are creating more prolific and rapid flows of information than ever before, it is little surprise that the Federal Government's Defence White Paper, released on 3 May 2013, emphasised cyber security as "a serious and pressing national security challenge" and a key priority.[1]

This latest White Paper demonstrates how the Government's approach to cyber security has evolved, since the last White Paper four years ago, to not only acknowledge the risks posed by cyber threats, but to recognise the benefits of exploiting cyberspace and establish a public-private framework to manage the risks and develop Australia's cyber capabilities.

The White Paper emphasises that the potential impact of cyber activity has grown as the Australian Defence Force (ADF) has become increasingly reliant on networked operations and vulnerable to cyber attacks. The White Paper states that, "In a future conflict or escalation to conflict, an adversary could use a cyber attack against Australia to deter, delay or prevent Australia's response or the ADF's deployment of forces" and that these attacks or intrusions could include the targeting of information systems, networks and other infrastructure that supports the ADF's decision-making and fighting capabilities.

The White Paper makes clear however, that despite the threats, the rise of "cyber power" has as many positives as it does negatives. While not defined in the White Paper, "cyber power" is a term increasingly used in military and technology circles to describe "the ability to use cyberspace to create advantages and influence events in [all] the …operational environments". f[2]

The effectiveness of Australia's developing cyber power capabilities are dependent on how well the Government exploits cyber capabilities through partnering with international and private domestic partners. The White Paper does not specify the role that the private sector partners will play in building Australia's strength in cyber security, but emphasis is placed on the Australian Cyber Security Centre (ACSC), which aims to facilitate improved interaction between government and industry partners.

The ACSC was identified in this year's National Security Strategy as the facilitator of "faster and more effective responses to serious cyber incidents" by bringing together the Government's security community in a single body.[3] Exactly how these partnerships will operate remains to be seen and the White Paper does not expand on how the ACSC will facilitate this interaction.

The White Paper diverges from the emphasis on "cyber warfare" in the 2009 Defence White Paper,[4] to place emphasis on a "whole-of-nation" approach to cyber security. It recognises that "Australia's national

[1] www.defence.gov.au/whitepaper2013/docs/WP_2013_web.pdf

[2] Dr. Stuart H. Starr, "Towards an Evolving Theory of Cyberpower" (2009) *NATO Cooperative Cyber Defence Centre of Excellence* website, http://www.ccdcoe.org/publications/virtualbattlefield/02_STARR_Cyberpower.pdf

[3] http://www.dpmc.gov.au/national_security/docs/national_security_strategy.pdf

[4] http://www.defence.gov.au/whitepaper2009/docs/defence_white_paper_2009.pdf

security, economic prosperity and social wellbeing now depend on the internet and the security of information". The White Paper also recognises that the security of commercial, government and private information is integral in ensuring confidence in Australia both domestically and internationally.

It is clear both from the White Paper and the National Security Strategy that the Government will need to determine how to effectively enforce legal frameworks within the digital environment. Both documents state that Australia will be working with international partners to promote a common understanding of existing international law as it applies to cyberspace, including the UN Charter and international humanitarian law.

This view that established principles of international law apply to cyberspace is a view shared by most countries. The approach echoes the views conveyed by the US Department of State,[5] that international law relating to armed conflict anticipates technological changes and contemplates that existing rules will apply to new technologies. The challenge for Australia and its international partners will therefore be to build certainty around how established legal principles apply to cyberspace.[6]

While there is clearly more to be done to boost Australia's cyber power, the White Paper demonstrates the evolution in the Government's approach to cyber security. Foreshadowed is the development of a comprehensive cyber partnership between Australia, the United States and the United Kingdom to address mutual threats emerging from cyberspace and of continued investment in cyber research, technology and analytical capabilities to ensure that Australia retains its edge in cyberspace. It will be interesting to see how the collaborative, partnership approach of the ACSC plays out in working towards these aims.

Contacts

Khai Dang
Partner
Sydney
T: +61 2 9258 6754
E: khai.dang@ashurst.com

Leah Jessup
Lawyer
Sydney
T: +61 2 9258 5608
E: leah.jessup@ashurst.com

[5] Harold Hongju Koh, Legal Advisor U.S. Department of State, "International Law in Cyberspace" (2012) Remarks at USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, MD, 18 September 2012, http://www.state.gov/s/l/releases/remarks/197924.htm

[6] http://www.state.gov/s/l/releases/remarks/197924.htm

The average internet user – from a judicial perspective

Google Inc v Australian Competition and Consumer Commission [2013] HCA 1
REA Group Ltd v Real Estate 1 Ltd [2013] FCA 559
Interflora Inc v Marks and Spencer Plc [2013] EWHC 1291 (Ch)

WHAT YOU NEED TO KNOW

- In Australia, recent decisions of the High Court and the Federal Court of Australia have shown that the "average internet user" is viewed as technologically advanced.
- The level of understanding of the Google search engine, attributed to the "average internet user" by the courts, makes it more difficult to successfully argue that Google's organic search results or sponsored links are misleading or deceptive.

The Australian High Court, UK High Court of Justice and Federal Court of Australia have delivered judgments this year in *Google Inc v Australian Competition and Consumer Commission* [2013] HCA 1 (6 February 2013) (*Google*), *Interflora Inc v Marks and Spencer Plc* [2013] EWHC 1291 (Ch) (21 May 2013) (*Interflora*) and *REA Group Ltd v Real Estate 1 Ltd* [2013] FCA 559 (7 June 2013) (*REA Group*).

Google search engine

As explained by French CJ, Crennan and Kiefel JJ in *Google*, when a user enters search terms into the Google search engine, it displays two types of search results: organic search results and sponsored links. Organic search results are ranked in order of relevance to the search terms entered by the user, as determined by the Google algorithm. Sponsored links are advertisements, which appear as determined by the Google AdWords program. Advertisers can "buy" keywords off Google, such that when a user searches for that keyword, an advertisement from the advertiser may be displayed. At the time *Google* was decided, sponsored links appeared either above the organic search results in a shaded yellow box or to the right of the organic search results in a white box. Both boxes were marked "Sponsored Links".

Legal issues

Google, *Interflora* and *REA Group* considered three related but distinctly different legal issues:

- whether a particular sponsored link is misleading or deceptive (*Google*; *REA Group*);
- whether Google itself has engaged in misleading or deceptive conduct by publishing a misleading or deceptive sponsored link (*Google*); and
- whether using a trade mark as a Google AdWords keyword per se is trade mark infringement by the advertiser (*Interflora*).

All three legal issues required the courts to define the current "average internet user".

Google

The High Court in *Google* agreed with the primary judge that the "relevant class" is people who would have:

- access to a computer connected to the internet;
- some basic knowledge and understanding of computers, the internet and the Google search engine;
- at least an elementary understanding of how the Google search engine works (but not a detailed familiarity);
- appreciated that Google was a commercial enterprise and had to generate revenue;
- read the sponsored links as a whole, including the URL, and would have expected to be taken to that URL upon clicking on the sponsored link;

- inferred that sponsored links are advertisements and are different from organic search results; and
- understood that sponsored links were messages from advertisers, which Google had not adopted or endorsed and was merely passing on for what they were worth.

Because Google did no more than represent that the sponsored links were advertisements, Google was found by the High Court to not have engaged in misleading or deceptive conduct.

REA Group

Bromberg J in *REA Group* followed the principles espoused by the primary judge and the High Court in *Google*. However, his Honour assigned a much greater degree of technical knowledge of the Google search engine to the "average internet user". For example, according to Bromberg J, the relevant class would have understood that:

- the prominence of a sponsored link depends on the payment made by the advertiser;
- the order of organic search results depends on the relevance of the website to the keywords searched for by the user, with the most relevant result appearing first;
- the organic search results are likely to be more relevant and reliable than sponsored links; and
- the content of the organic search results is taken from the website and is not authored by the Google search engine.

Because the relevant class possessed this knowledge, his Honour found that the vigilance of an internet user would increase the further that user moves down the list of organic search results (such that small differences in the URL in low-ranked results would be more noticeable to the user than the same differences appearing in the first few results). This was relevant in *REA Group*, because the alleged misleading or deceptive organic search results appeared on page 5 of the search results, and therefore were held to be unlikely to mislead or deceive.

Interflora

Compared to the approaches of the High Court and Federal Court of Australia, the UK High Court of Justice viewed the "average internet user" as rather technologically illiterate.

Arnold J found that the average reasonably well-informed and observant internet user is broadly aware that there is a distinction between organic search results and sponsored links. However, his Honour still believed that "*a significant proportion*" would not appreciate that sponsored links appear "*because the advertisers have paid for the advertisements to be triggered by a keyword consisting of or related to the search term entered by the user.*"

Changes to the Google search engine since these decisions

Since the *Google* decision, Google has revised its AdWords trade mark policy such that it will no longer prevent customers from using a third party's trade mark as a keyword in advertisements. This means that trade mark owners will now have to contact the advertiser if they believe that a sponsored link is misleading, rather than making a complaint to Google.

In addition, there has been a change to the layout of the search engine since *Google*. The sponsored links are now marked "Ads related to [search term]" (above the organic search results) and "Ads" (to the right of the organic search results). This change makes it clear to internet users that sponsored links are advertisements. However, Google has also removed the shaded yellow box, making it more difficult to distinguish the end of the sponsored links from the start of the organic search results. Arguably, this second change could have altered the outcome in *Google*. This is because, as the primary judge noted, "*the shaded rectangular box draws attention not only to the advertisements appearing within it but also to the words "sponsored links" appearing in its upper right hand corner*".

Contacts

Gordon Hughes
Partner
Melbourne
T: +61 3 9679 3395
E: gordon.hughes@ashurst.com

George McCubbin
Graduate
Melbourne
T: +61 3 9679 3499
E: george.mccubbin@ashurst.com

Council captured in CCTV privacy breaches

SF v Shoalhaven City Council [2013] NSWADT 94

WHAT YOU NEED TO KNOW

- In response to the New South Wales Administrative Decisions Tribunal's decision, the NSW Government has amended the PPIP Regulations to specifically exempt council CCTV programs from certain IPPs.

WHAT YOU NEED TO DO

Councils using CCTV cameras for the purpose of crime prevention should ensure:

- any personal information recorded is relevant to the purpose of crime prevention;
- the signage alerting people to the presence of CCTV cameras is sufficient to meet their privacy obligations;
- the footage is of sufficient quality to be useful in preventing crimes (for example, faces and numberplates can be identified); and
- adequate safeguards are in place against the loss, unauthorised access and misuse of personal information.

In *SF v Shoalhaven City Council* [2013] NSWADT 94, the New South Wales Administrative Decisions Tribunal ruled that the Shoalhaven City Council's (Council) CCTV program contravened the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act). The Tribunal did not accept that the Council's CCTV program was exempt for "law enforcement purposes", concluding that the Council was required to comply with the Information Protection Principles (IPPs) set out in the PPIP Act for any personal information it collected as part of its CCTV program.

In response to the Tribunal's decision, the NSW Government amended the PPIP Regulations to specifically exempt council CCTV programs from certain IPPs.

The Application for Internal Review

The Council operates its CCTV cameras 24 hours a day within the Nowra CBD. The images are streamed live to a monitor, and stored on a hard drive, at the Nowra Police Station. Signs are located within the vicinity of the cameras to alert people of their presence.

An application for Internal Review was brought by a resident of Nowra who claimed that the collection and storage of his personal information through the Council's CCTV program breached the IPPs.

The IPPs govern the collection, use, disclosure, access and storage of personal information by public sector agencies in New South Wales. Public sector agencies collecting personal information must take reasonable steps to ensure that:

- individuals are aware that their information is being collected and the purpose of the collection;
- the information is relevant to the purpose, accurate, up to date, complete and not excessive;
- the information is secured against loss and unauthorised access, use or disclosure; and
- individuals can ascertain whether their personal information is held by the public sector agency and gain access to the information.

The Applicant claimed the collection of his personal information was not relevant to the Council's purpose of crime prevention because the CCTV program had not been successful in preventing crime, less than one per cent of the personal information gathered related to crime prevention and the footage was of such poor quality that offenders were unlikely to be identified.

The decision

The Tribunal ruled that the Council's use of CCTV cameras was lawful as it was directly related to the Council's crime prevention functions or activities.

However, the Council was not exempt from complying with the IPPs because the information was not collected for a "law enforcement purpose" .

The Tribunal found that the Council contravened IPPs 10, 11 and 12(c). The signs alerting people to the presence of the CCTV cameras provided insufficient details about the collection of their personal information, the collection was excessive, inaccurate and incomplete and the information was not adequately secured against loss, unauthorised access and misuse.

Implications for other councils

In other Australian jurisdictions, public sector agencies must comply with legislated information privacy principles that cover similar ground to the NSW IPPs.

In response to concerns by NSW councils following the Tribunal's decision, the NSW Government amended the PPIP Regulations to specifically exempt council CCTV programs, in certain circumstances, from IPPs 11 and 18. These IPPs limit the disclosure of collected information and ensure it is relevant to the purpose of collection, not excessive, accurate, up-to-date, complete and not unreasonably intrusive.

These changes will not deter privacy advocates who argue that CCTV programs installed by councils for crime prevention purposes should prevent crime, be fit for the purpose of crime prevention and comply with existing privacy laws.

Councils using CCTV cameras for the purpose of crime prevention should ensure:

- any personal information recorded is relevant to the purpose of crime prevention;
- the signage alerting people to the presence of CCTV cameras is sufficient to meet their privacy obligations;
- the footage is of sufficient quality to be useful in preventing crimes (for example, faces and numberplates can be identified); and
- personal information is secured against loss, unauthorised access and misuse.

Contacts

Amanda Ludlow
Partner
Brisbane
T: +61 7 3259 7164
E: amanda.ludlow@ashurst.com

Sophie Hollier
Senior Associate
Brisbane
T: +61 7 3259 7003
E: sophie.hollier@ashurst.com

Ffion Whaley
Graduate
Brisbane
T: +61 7 3259 7577
E: ffion.whaley@ashurst.com

Telstra's quest for quality of service in rural areas

Telstra Corporation Limited v Indigo SC [2013] VCAT 659 (1 May 2013)

WHAT YOU NEED TO KNOW

The Tribunal recognised that:

- telecommunications providers are in the best position to understand how networks operate across a region and where there is a need for additional infrastructure, and.
- persons in rural areas have a right to have a quality of service equal to that of regional centres, when available.

On 1 May 2013, the Victorian Civil and Administrative Tribunal (Tribunal) set aside the decision of the Responsible Authority, Indigo Shire Council (Council) to refuse a permit to Telstra Corporation Limited (Telstra) for the development of a telecommunications tower in Victoria. Prior to the hearing, in private negotiations, the Council consented to an amended form of the proposal. The Respondents in this action are represented by Michael Bell, on behalf of other concerned parties. The Tribunal ultimately allowed the permit to be issued, subject to a number of conditions.

The Tribunal considered a number of policies under the *Code of Practice for Telecommunications Facilities in Victoria* (Code) as well as balancing the public interest of local residents and environmental concerns.

Telstra submitted that the proposed telecommunications tower is *needed* in the particular rural area as there is patchy coverage due to terrain obstructions and the distance between existing base stations. Telstra noted that if the permit was approved, expected enhancements would include improved depth of coverage, faster wireless speeds, more consistent signals, fewer drop outs, superior emergency notifications and the ability to use the full range of mobile services reliably.

The Respondents submitted evidence that the position was already improved from the erection of a telecommunications tower post the Black Saturday Bushfires and that there was no need for the additional tower. While the Code does not require "need" as a factor, it does recognise the importance of modern communication and the need to provide infrastructure to allow service to be made available to all sections of the community. That being said, it is relevant that the policy underlying the Code gives encouragement to these types of facilities. The Tribunal found that service providers are the best placed to understand how the network operates across a region, where gaps exist, where service quality is poor, and what complaints are being received from users or prospective users. In doing so, they also considered the public interest, in that, the level of service in both regional and rural locations should not vary significantly and where possible, be commensurate.

The proposal was initially refused by the Council on grounds that Telstra had not satisfactorily ascertained whether there was an available co-location. While the Council now supports the amended proposal (which involved painting the structure a neutral colour and moving the site 50 metres), the Respondents brought this question to the Tribunal. The Tribunal was satisfied that co-location options had been explored and found unsuitable.

The Respondents also made submissions that the presence of the proposed tower would be an unacceptable visual intrusion to the surrounding landscape and natural features of the area (particularly the panoramic view between Baranduda and Murramurrangbong ranges), as well as be highly visible and unreasonably dominant.

The Tribunal assessed the location of the base tower and State policies regarding environmental protection, and, while agreeing that the landscape character and quality are part of the site's context, the Tribunal rejected argument that the telecommunications tower would obstruct or influence the heritage areas which were a substantial distance away. While visually the telecommunications tower would be obvious (being

approximately 37 metres above ground level), the Tribunal did not find it to be unacceptable.

The Tribunal noted that while a viewer with particular sensitivity to the structure may find the presence of the tower unattractive or intrusive, overall it would not be unreasonably dominant. In order to minimise any issues, the Tribunal ordered that the facility be "finished" in a pale eucalypt colour to minimise the visual impact of the structure.

The Tribunal, as urged by the Respondents, also considered the alleged health impact of the telecommunications tower and the associated electromagnetic radiation. The Tribunal noted these concerns and noted as a condition to the permit, that the facility must be designed and installed so that the maximum human exposure levels to radio frequency emissions comply with Australian Standard AS/NZS 2772.1:1999.

The Tribunal ordered that the Council's decision be set aside, and that Telstra be issued with a permit subject to various conditions. In addition to those noted above, there must be a vegetation screen of 20 metre depth radiating from the perimeter, a landscape plan approved by the Council, and upon cessation of the facility, the structures must be removed from the site and the land rehabilitated to the standard of the land prior to occupancy.

Contacts

Khai Dang
Partner
Sydney
T: +61 2 9258 6754
E: khai.dang@ashurst.com

Jessica Norgard
Lawyer
Sydney
T: +61 2 9258 6564
E: jessica.norgard@ashurst.com

"There is also a question of equity whereby the level of service in locations such as the review site should not vary significantly from, for example, major regional centres where reception and data access is generally currently better, more reliable and faster."

A warning to telecommunications service providers about the use of telemarketers

ACCC v Excite Mobile Pty Ltd [2013] FCA 350

WHAT YOU NEED TO KNOW

- The ACCC is cracking down on unconscionable and misleading and deceptive conduct engaged in by telemarketers on behalf of telecommunications service providers.

WHAT YOU NEED TO DO

- Whilst the conduct of the service provider in this case was particularly egregious, it warns against basic mistakes by telemarketers – such as misrepresenting coverage and not properly informing customers.

The Federal Court of Australia recently gave consideration to the conduct of telemarketers in *ACCC v Excite Mobile Pty Ltd* [2013] FCA 350.

Trade Practices Act

The case concerned the behaviour of a mobile telephone services provider, Excite Mobile. Excite Mobile was found to have breached the *Trade Practices Act 1974* (Cth) (the Act), which was in force at the time of the alleged acts and omissions, because:

1. Excite Mobile engaged in unconscionable conduct by adopting an inappropriate telemarketing sales method (section 51AB of the Act). Mansfield J found that the service offered by Excite Mobile was unusual and not suited to the everyday user. However, the sales pitch "*only fleetingly*" explained the unusual feature and the telemarketing process was "*pushy*" and gave the consumer little time for thought or for questions. His Honour remarked that "*It was unfair to such a degree as to attract a strong adverse moral judgment*".

2. Excite Mobile engaged in misleading and deceptive conduct by misrepresenting the coverage available to customers (sections 52 and 53(c) of the Act). In 16 cases, Excite Mobile's telemarketers incorrectly represented that the customer had mobile coverage at their home addresses. It was irrelevant that the misrepresentations were caused by "*human error*" in checking the coverage.

3. Excite Mobile engaged in misleading and deceptive conduct by representing to consumers that the "Telecommunications Industry Complaints" (TIC) body, where Excite Mobile's customers were referred to for complaints, was an independent body (sections 52 and 53(g) of the Act). TIC was, in fact, affiliated with Excite Mobile and created to avoid customers making complaints to the Telecommunications Industry Ombudsman.

4. Excite Mobile engaged in misleading and deceptive conduct, unconscionable conduct and undue coercion by creating a fictitious debt collector, called Jerry Hastings, to contact Excite Mobile's debtors (sections 51AB, 52, 53(g) and 60 of the Act). "Jerry Hastings" used strong and threatening language, in order to "*intimidate all but the well informed or well experienced debtor into responding to them*". The letters falsely asserted that a court would order extra charges for outstanding debts and repossession of all assets of the debtor. For example, one of the standard form letters from "Jerry Hastings" included the following statement:

> *Believe me there is no way you want to meet my lawyer in court. While she seems like a nice lady she is a killer in front of the judge. One case she even got the judge to order a young mother have her kids game machine repossessed. She has no feelings towards you at all. Her job is to be as mean as possible towards you. She can make your life extremely uncomfortable.*

Personal liability

Excite Mobile's directors, Mr Brown and Mr Samuel, and an agent of Excite Mobile, Ms Smart, were also found to be liable for the breaches of the Act. Mr Brown was responsible for the operations of Excite Mobile and was found to be involved in and knowingly concerned in all of the breaches. Ms Smart sent the "Jerry Hastings" letters and was found to have been knowingly involved in the misleading conduct.

Mr Samuel was a director of Excite Mobile, but he argued that he was only "*nominally involved*" in its operations. Mansfield J disagreed saying, "*I think that over time he has come to view his role in Excite Mobile as somewhat less than it was*". It was sufficient for accessorial liability for Mr Samuel to have been aware of, and to have supported, the use of the sales script and "Jerry Hastings" letters.

A warning about telemarketers

Mansfield J was highly critical of the telemarketing used by Excite Mobile. His Honour suggested that "*[i]t may be appropriate to consider whether … the supplier should be required to give to the consumer the opportunity to listen to the recorded interview upon which the contract is said to arise*" before the contract is formed.

Another telecommunications service provider was recently the subject of ACCC investigations. On 4 June 2013, Utel Networks Pty Ltd paid three infringement notices, costing it $19,800, to the ACCC for conduct including making false or misleading representations to consumers about the quality of the service they would receive upon being transferred to Utel Networks. As the ACCC Commissioner Sarah Court said in relation to the Utel Networks investigation, "*The ACCC will continue to hold companies responsible for what is said or done by their authorised representatives. Lack of oversight by businesses will not be accepted as a valid excuse for misleading consumers.*"

Contacts

Gordon Hughes
Partner
Melbourne
T: +61 3 9679 3395
E: gordon.hughes@ashurst.com

George McCubbin
Graduate
Melbourne
T: +61 3 9679 3499
E: george.mccubbin@ashurst.com