Communications Law BULLETIN

CAMLA

Communications & Media Law Association Incorporated

Print Post Approved PP: 100001546

Consumer Protection Enforcement Update:
Spotlight on Telecommunications Industry

Recent regulatory changes have seen a range of new measures introduced to assist consumers in their dealings with telecommunications service providers. Bruce Lloyd, Matthew Battersby and Alexia Takis take a look at the growing willingness of the ACCC and the ACMA to take enforcement action to change advertising, disclosure and sales practices in the industry.

Introduction

Consumer protection in the telecommunications sector continues to be a focus area for Australian regulators. The Australian Competition and Consumer Commission (***ACCC***) and the Australian Communications and Media Authority (***ACMA***) have both signalled that enforcement action will be taken using formal warnings, infringement notices, court enforceable undertakings and pecuniary penalty proceedings, in addition to education and compliance efforts.

In February, ACCC Chairman Rod Sims released the ACCC's updated Enforcement and Compliance Policy and announced the ACCC's priorities for 2013[1], with "consumer protection in the telecommunications and energy sectors" at the top of its list.[2] Looking ahead, the more traditional focus on misleading and deceptive conduct, particularly in advertising, is likely to continue. New provisions in the Australian Consumer Law (***ACL***) dealing with unfair contracts, unsolicited consumer agreements and consumer guarantees commenced on 1 January 2011 and are also starting to receive particular attention.

In addition, the ACMA registered the Telecommunications Consumer Protections Code 2012 (***TCP Code***) just over a year ago. The TCP Code was developed in partnership with the industry and contains some prescriptive requirements on carriage service providers designed to improve advertising and sales practices, minimise bill shock, and address confusing mobile plans and poor complaints-handling practices.

One of the key objectives behind the focus on consumer protection by the ACCC and the ACMA is a desire to improve the level of transparency and disclosure in the industry to avoid consumer confusion and provide sufficient information for consumers to make an informed decision when purchasing products or services. The ACL and TCP Code are the principal regulatory and enforcement tools used to achieve this objective.

This article explores some of the recent consumer protection matters which have been pursued by the ACCC and the ACMA and considers the implications for telecommunications service providers.

---

1 Rod Sims, "The ACCC's 2013 Priorities" (Speech delivered at the Committee for Economic Development of Australia, Sydney, 21 February 2013).

2 ACCC, *Compliance and Enforcement Policy* (February 2013).

Volume 32 Nº 4
October 2013

Inside This Issue:

SAVE THE DATE
Thursday 28 November

The Communications and Media Law Association invites members to the Annual General Meeting and End of Year Drinks

More details on page 14

Contents

Advertising and Disclosure

The rapid take-up of smartphones and internet plans has caused the ACCC and the ACMA to focus closely on advertising standards in the telecommunications sector. Both regulators have expressed concerns about the level of transparency and disclosure in advertisements and have taken action where they perceive a risk of consumer harm.

regulators have expressed concerns about the level of transparency and disclosure in advertisements

Truth-in-Advertising Undertaking

Looking back to 2009, Telstra, Optus and Vodafone gave a court-enforceable undertaking to the ACCC to "set a new industry benchmark for 'truth in advertising'" in response to a "significant number of complaints" received by the ACCC about advertising and promotional practices in the industry (***Truth-in-Advertising Undertaking***).[3] The Truth-in-Advertising Undertaking has now expired, but contained commitments from the three carriers that they would not engage in specific advertising practices which the ACCC considered were likely to mislead or deceive consumers.

TCP Code

Many of the specific advertising restrictions contained in the Truth-in-Advertising Undertaking can now be found in Chapter 4 of the TCP Code which commenced on 1 September 2012 and has been progressively phased in over the last 12 months.[4] The TCP Code is a mandatory industry code registered under Part VI of the *Telecommunications Act 1997* (Cth) and applies to carriage service providers who supply telecommunications products to residential and some small business customers.

The TCP Code contains some prescriptive requirements designed to improve transparency and disclosure. These include rules for the use of headline representations, disclaimers, price representations and terms such as "unlimited", "free", "cap", "no exceptions", "no exclusions" or "no catches".[5] The TCP Code also contains mandatory disclosure requirements, which require carriage service providers to:

- prepare a two page "Critical Information Summary" for current pre-paid and post-paid plans which must be made available online and in store;[6]
- prominently disclose in any advertisement containing the price or dollar value of a post-paid plan the cost of a two-minute standard national call, a standard SMS and using 1MB of data within Australia;[7] and
- issue notifications to consumers with post-paid plans or data plans when usage of their included value allowance (for voice, SMS and data) reaches 50, 85 and 100 per cent.[8]

The ACMA is focused on TCP Code compliance and has issued formal warnings or directions to comply to several service providers in the past year, including Touch Mobile and Vodafone.

Australian Consumer Law

In addition to the specific requirements in the TCP Code, the ACL contains general prohibitions on misleading or deceptive conduct in relation to goods or services (sections 18, 29, 33 and 34) and requires suppliers to specify the single price of consumer products in a prominent way and as a single figure (section 48). These provisions of the ACL apply to conduct "in trade or commerce" such as advertising, sales and post-sales practices.

The ACCC is responsible for enforcing the ACL and has commenced court proceedings against a number of telecommunications service providers over the years, including Telstra, Optus and TPG, in relation to advertisements which it believes contravene the ACL and its predecessor provisions in the *Trade Practices Act 1974* (Cth) (***TPA***).[9]

In recent times, the ACCC has taken a stronger stance on conduct which it considers may mislead consumers and has commenced pecuniary penalty proceedings or issued infringement notices to several telecommunications service providers. The case studies below show that the ACCC has focused on headline representations, component pricing and the adequacy of disclaimers.

---

3 Telstra Corporation Limited, Singtel Optus Pty Limited, Vodafone Hutchison Australia Pty Limited, *Undertaking to the Australian Competition & Consumer Commission given for the purposes of section 87B* (14 September 2009).

4 Although some rules have had a delayed implementation date, the majority of the key obligations under the TCP Code have now commenced.

5 *Telecommunications Consumer Protections (TCP) Code* (C628:2012), cl 4.2.

6 TCP Code, cl 4.1.2.

7 TCP Code, cl 4.2.6.

8 TCP Code, cl 6.5.2. Smaller service providers (less than 100,000 customers) have an additional 12 months before they are required to issue SMS/voice usage notifications. All service providers must provide data notifications from 1 September 2013.

9 *Australian Competition and Consumer Commission v Telstra Corporation Limited* [2007] ATPR 42-207; [2007] FCA 2058.

Case study: ACCC v Singtel Optus Pty Ltd (March 2012)

The ACCC commenced proceedings against Optus in September 2010 alleging misleading claims about download allowances in Optus' "Think Bigger" and "Supersonic" broadband internet plan advertisements. The advertisements marketed a cap on peak and off-peak downloads and contained a disclaimer stating that "speed limited once peak data exceeded". Once the peak quota was used up, the speed of the service was shaped irrespective of the usage of the off-peak or overall quotas.

The ACCC took issue with advertisements promoting the plans over a 5 month period. Justice Perram agreed at first instance and fined Optus $5.26 million for 11 contraventions of section 55A of the TPA (now section 34 of the ACL).[10] In March 2012, the Full Federal Court reduced this penalty to $3.61 million.[11]

Case study: ACCC issues infringement notice to iiNet Limited (June 2013)

In June 2013, iiNet paid a $102,000 infringement notice in relation to advertisements for iiNet's Naked DSL Service which the ACCC considered did not *prominently* display the total minimum price payable for the service, as required by section 48 of the ACL. The $1,518.75 total price over 24 months was displayed towards the bottom of the advertisement and in font smaller than the $59.95 monthly payment.

Case study: ACCC v TPG Internet Pty Ltd (ongoing)

In September 2010, TPG commenced an $8.9 million multi-media advertising campaign promoting an unlimited ADSL2+ broadband service for $29.95 per month where a consumer bundled this with a home phone service for a total of $59.95 per month. The bundling condition, setup charges and total cost over the life of the contract were displayed less prominently than the headline $29.95 representation.

Despite modifying its initial advertisements in response to ACCC concerns, the ACCC commenced proceedings against TPG in December 2010 alleging that its advertising campaign was misleading. The trial judge agreed and fined TPG $2 million for contraventions of sections 18 and 29 of the ACL and the TPA predecessors of sections 18, 29 and 48 of the ACL.[12] TPG appealed and was largely successful, with the Full Federal Court finding that only some initial advertisements (which ran for 12 days prior to the ACCC raising concerns with TPG) were misleading. In April 2013, the Full Federal Court reduced the pecuniary penalty to $50,000, set aside the injunction, corrective advertising and compliance program ordered by the trial judge and ordered the ACCC to pay 75% of TPG's costs.[13]

The Full Court emphasised that the "overarching rule" or "critical question" which must be examined is whether the whole of the advertisement in its full context was misleading, and not just the dominant message conveyed by the advertisement. The Court held that the full context included consumer knowledge about "the 'bundling' method of sale commonly employed with this type of service, as well as knowledge that setup charges are often applied".[14]

In August 2013, the High Court granted the ACCC special leave to appeal the Full Federal Court's decision.

Broadband Speed Claims

The ACCC announced in August 2013 that it is considering implementing a broadband performance monitoring and reporting program to examine actual broadband speeds available to consumers and compare them with headline speed claims by internet service providers.[15]

The ACCC has in the past expressed concerns about the marketing of broadband speeds and has published several information papers outlining its expectations of internet service providers.[16] The ACCC considers that the proposed monitoring program would:

- provide transparency and allow consumers to compare broadband services based on real-world performance rather than theoretical maximum speed claims;
- hold internet service providers accountable for performance claims, including headline speed claims; and
- encourage competition and efficient investment in infrastructure.

the "overarching rule" is whether the whole of the advertisement in its full context was misleading, and not just the dominant message conveyed by the advertisement

Fixed-line, fixed wireless and satellite broadband services would be examined initially with the option to add mobile broadband services at a later date. The ACCC is currently seeking feedback from the industry, consumer groups and other stakeholders on an appropriate program design, including the testing methodology, scope, quality of service metrics and reporting framework.

While the results of the broadband performance monitoring program may aid transparency, it indicates there will be special scrutiny of broadband performance claims and could result in further enforcement action by the ACCC where the results do not substantiate representations made in advertisements. The ACCC is warning that:

> if there was evidence of a network operator over-promising and under-delivering the ACCC could consider enforcement action for misleading and deceptive conduct and/or for failure to comply with any applicable regulatory determinations.[17]

Unfair Contracts

A new prohibition on unfair contract terms commenced with the introduction of the ACL and enforcement of these new provisions is a current priority for the ACCC. The ACL states that a term in a standard form consumer contract will be void if it is unfair; that is it would cause a significant imbalance in the parties' rights and obligations, is not reasonably necessary in order to protect the legitimate interests of the party, and it would cause detriment (financial or otherwise) to a party if it were to be relied upon.[18]

Standard form consumer contracts are used extensively to supply retail telecommunications services. The ACCC recently conducted

---

10 *ACCC v Singtel Optus Pty Ltd (No. 4)* [2011] FCA 761.

11 *Singtel Optus Pty Ltd v ACCC* [2012] FCAFC 20.

12 *Australian Competition and Consumer Commission v TPG Internet Pty Ltd* [2011] ATPR 42-383; [2011] FCA 1254; *Australian Competition and Consumer Commission v TPG Internet Pty Ltd (No 2)* [2012] ATPR 42-402; [2012] FCA 629.

13 *TPG Internet Pty Ltd v Australian Competition and Consumer Commission* (2012) 201 FCR 277; [2012] FCAFC 190; *TPG Internet Pty Ltd v Australian Competition and Consumer Commission* [2013] ATPR 42-432; [2013] FCAFC 37.

14 *TPG Internet Pty Ltd v Australian Competition and Consumer Commission* (2012) 201 FCR 277; [2012] FCAFC 190 at [105].

15 ACCC Consultation Paper, "Broadband performance monitoring and reporting in the Australian context" (14 August 2013).

16 See for example ACCC Information Paper, "HFC and Optical Fibre Broadband "Speed" Claims and the Competition and Consumer Act 2010" (July 2011).

17 ACCC Consultation Paper, "Broadband performance monitoring and reporting in the Australian context" (14 August 2013) at page 3.

18 *Australian Consumer Law,* ss 23, 24. Section 25 of the ACL provides some examples of the kinds of terms that could be considered to be unfair.

a review of standard form contracts and published its findings in March 2013. This review identified contract terms which the ACCC considered were of particular concern (e.g. unilateral change rights, unfair restrictions on termination). [19] The telecommunications sector was a target and terms in TPG and Dodo's standard form contracts are discussed in the ACCC's report.

Case study: ACCC v ByteCard Pty Ltd

The first case brought exclusively under the unfair contract terms provisions was against internet service provider ByteCard Pty Limited (trading as NetSpeed Internet Communications). The ACCC commenced proceedings in April 2013 alleging that a number of ByteCard's standard terms were unfair and should be declared void. The terms in question:

- allowed ByteCard to unilaterally change prices without giving the consumer a right to terminate the contract;
- required the consumer to indemnify ByteCard in circumstances where the consumer had not breached the contract and ByteCard may have caused the loss; and
- gave ByteCard the right to unilaterally terminate the contract at any time without cause or reason and without giving compensation to the consumer.

On 24 July 2013, the Federal Court made declarations that the terms were unfair and therefore void under the ACL and ByteCard was ordered to pay $10,000 towards the ACCC's costs.

Unsolicited Consumer Agreements

The ACCC has been active in the enforcement of the unsolicited consumer agreement provisions of the ACL. These provisions govern door-to-door sales and telemarketing and include specific requirements about documenting the agreement[20] and ensuring that sales staff:

- obey permitted calling hours;[21]
- disclose their purpose and identity prior to negotiating and provide consumers with information about their termination rights prior to an agreement being made;[22] and
- leave premises immediately upon request.[23]

Retail electricity and gas providers have been the focus of ACCC enforcement action to date,[24] however, any inappropriate telemarketing or door-to-door sales practices of telecommunications service providers will be targeted in the future given the ACCC's current priorities.

Case study: Utel Networks Pty Ltd

In June 2013, for example, Utel Networks Pty Ltd paid infringement notices totalling $19,800 and gave the ACCC an enforceable undertaking in relation to its telemarketing practices. The ACCC alleged that Utel personnel made false representations that Utel was affiliated with Telstra (when it was not) and that the quality of service would not change if consumers switched from their current service provider to Utel. The ACCC also alleged that Utel did not provide consumers with compliant agreement documentation containing notice on the front page clearly informing consumers of their termination rights.[25]

Consumer Guarantees

Part 3-2 of the ACL contains non-excludable statutory consumer guarantees which provide consumers with a basic, guaranteed level of protection for goods and services they acquire. Consumers supplied with goods or services that fail to meet the consumer guarantees are entitled to certain remedies under Part 5-4 of the ACL depending on whether the failure is major or minor. These remedies include a repair, replacement or refund.

The interaction between the statutory consumer guarantees regime and voluntary express warranty offered by device manufacturers has caused compliance issues for a number of telecommunications suppliers, particularly in relation to mobile phones. Optus and Vodafone have both given enforceable undertakings following concerns raised by the ACCC about how they were dealing with consumer complaints about faulty devices.[26] Businesses risk breaching the general prohibition on misleading and deceptive conduct under the ACL if they make false representations about the application of the consumer guarantees or the statutory remedies to which a consumer is entitled.

Case study: ACCC v Hewlett-Packard Australia Pty Ltd

The ACCC alleged that HP made misleading representations to consumers about their statutory guarantee rights over a 21-month period, including that:

- remedies were limited to those provided by HP at its discretion;
- HP products needed to be repaired multiple times before consumers were entitled to a replacement;
- the warranty period for HP products was limited to a specified express warranty period;
- consumers were required to pay HP to repair products not of acceptable quality; and
- consumers could only return HP products purchased from HP's online store at the sole discretion of HP.

The Federal Court found HP liable for 6 contraventions of section 29(1)(m) of the ACL and, by consent, imposed a $3 million pecuniary penalty, $200,000 towards the ACCC's costs, an injunction and corrective advertising orders among others.[27]

Conclusion

The regulatory regime governing dealings between telecommunications service providers and consumers is comprehensive. The ACCC and the ACMA have both devoted significant resources to consumer protection and have shown a willingness to use their extensive armoury of enforcement tools, including pecuniary penalty proceedings in the Federal Court and infringement notices where they perceive a risk of consumer harm. The focus by these regulators on business practices in the telecommunications sector reinforces the need for a strong compliance and advertisement clearance program addressing matters under the ACL and the TCP Code to avoid penalties of up to $1.1 million per ACL contravention and $250,000 per TCP Code contravention.

Bruce Lloyd is a partner and Matthew Battersby and Alexia Takis are lawyers in the Competition team at Clayton Utz.

---

19 ACCC Report, *Unfair Contract Terms - Industry Review Outcomes* (March 2013).

20 *Australian Consumer Law,* ss 78 - 81.

21 *Australian Consumer Law,* s 73.

22 *Australian Consumer Law,* ss 74, 76.

23 *Australian Consumer Law,* s75.

24 See *Australian Competition and Consumer Commission v Neighbourhood Energy Pty Ltd* [2012] ATPR 42-426; [2012] FCA 1357 (Neighbourhood Energy was ordered to pay $850,000 and its marketing company Australian Green Credits Pty Ltd was ordered to pay $150,000). In March 2012, the ACCC commenced proceedings against AGL Sales Pty Ltd, AGL South Australia Pty Ltd and AGL's marketing company CPM Australia Pty Ltd. In May 2013, Middleton J made orders for pecuniary penalties: AGL was fined $1,555,000 and CPM was fined $200,000. In March 2013, the ACCC commenced proceedings against Energy Australia Pty Ltd and its marketing company and in September 2013 it commenced proceedings against Australian Power & Gas Company and Origin Energy.

25 *Australian Consumer Law,* s79(b).

26 Optus Mobile Pty Limited, *Undertaking to the Australian Competition & Consumer Commission given for the purposes of section 87B* (6 January 2011); Vodafone Hutchison Australia Pty Limited, *Undertaking to the Australian Competition and Consumer Commission given for the purposes of section 87B* (12 January 2010).

27 *Australian Competition and Consumer Commission v Hewlett-Packard Australia Pty Ltd* [2013] FCA 653.

Champing at the Bitcoin: Bitcoin, Regulators and the Law

David Rountree gives an overview of the history of Bitcoin and recent attempts by regulators to deal with this perplexing phenomenon.

Introduction

Welcome to the world of Bitcoin – where banks are obsolete, governments are circumvented and currency goes online. No need for those pesky coins filling your wallet, or even that cumbersome credit card. Now your money can exist entirely in an abstract world, protected by the power of a like-minded community, cryptography, and really complicated maths. This is the brave new world that Bitcoin promises.

Bitcoin is an online digital currency which exists and is stored solely on the internet. Bitcoin is not backed by any asset or linked to any organisation – in fact it exists completely independently of any organisational structure. Bitcoins can currently be used to purchase goods and services, as well as be exchanged for other mainstream currencies.

But where does the law fit in? This article aims to take a brief look at Bitcoin, its history, and how the law and regulators have attempted to deal with it in its brief (and slightly chequered) history. This has recently been given some clarity due to the US Federal Court decision of *Security Exchange Commission v Trenders T Shavers and Bitcoin Savings and Trust*.[1]

What is Bitcoin?[2]

Bitcoin has a number of unique features which distinguishes it from other "mainstream" currencies.

No central bank to print or produce currency - mining

Firstly, there is no centralised bank, such as the Reserve Bank of Australia, which processes, verifies and produces bitcoins. Bitcoins cannot be simply printed like regular money. In fact, in a process designed to mirror the discovery of precious metals, Bitcoins are produced by a process called "bitcoin mining".

A Bitcoin is "mined" on a computer, which by running a program is asked to solve a complex 64 digit algorithm. Successfully solving this algorithm is rewarded by the "miner" receiving 50 bitcoins.

An important feature of bitcoins is that they are finite – the algorithm that produces them will only produce $21 million bitcoins.[3] They are designed to release at a steady rate, but provide diminishing returns, as the algorithm gets increasingly difficult to solve as more bitcoins are mined. Recent figures suggest roughly half of the bitcoins have been extracted, with the production expected to peter out over the next decade until the virtual bitcoin mine is exhausted.

No intermediate financial institution – peer to peer system

Bitcoins are also unique in that there is no need for an intermediate financial institution to transfer them and verify them. In this way, they operate similar to cash. Transactions are processed and verified not by a bank, but by the processing power of computers engaged in mining. The act of mining bitcoins also involves confirming waiting transactions. All transactions on the Bitcoin network are recorded and shared across the network, which are then recorded as part of the mining in the "block chain". The complex mathematical formula is then reinforced by security mechanisms, preventing people replicating or double spending individual bitcoin.

This lack of involvement from government and financial institutions also contributes to another key feature of Bitcoin – their anonymity. Indeed Bitcoin has been heavily associated with the "Silk Road", an online marketplace from which one can purchase a variety of illegal goods. Bitcoin's anonymity has made it the currency of choice of Silk Road sellers, as well as a useful medium for both money laundering and financial schemes. This in turn has attracted the interest of law enforcement and regulators, which is addressed below.

Bitcoin is not backed by any asset or linked to any organisation – in fact it exists completely independently of any organisational structure.

History of Bitcoin

Bitcoins first hit the internet in 2008, as the subject of a paper by a user by the name of Satoshi Nakamoto, entitled "Bitcoin: A Peer to Peer Electronic Cash System".[4] The first 25 coins, known as the "Genesis Block", were mined in 2009. Since that time, Bitcoin has gathered momentum, at first slowly, and then incredibly rapidly.

At its inception, a bitcoin was virtually worthless,[5] and while the first Bitcoin market was established in February 2010, its value compared with regular currency remained minimal. It was limited to what it could buy, which at this stage was very little. However, it slowly gathered traction, and in February 2011 a bitcoin was equal to a US dollar on a Bitcoin exchange.

Since that time, things rapidly became interesting for Bitcoin.

First, its founder, Mr Nakamoto, who had also contributed heavily in online forums to the technical literature surrounding Bitcoin, vanished without a trace. All efforts to discover the true identity of this user have so far proved fruitless.[6]

Secondly, there was a marked jump in interest in bitcoins. The mainstream internet became more aware of this idea, reputable online retailer began accepting it, and buzz was generated. This buzz even captured the imagination of the Cameron and Tyler Winklevoss

1 Memorandum of Opinion Regarding Courts Subject Matter Jurisdiction, Case No 3:13-CV-416 (Eastern District of Texas, Sherman Division) (***SEC v Shavers***)

2 Technical explanations regarding the operation of Bitcoin can be found in a number of places, including http://www.weusecoins.com/en/; http://bitcoin.org/en/how-it-works; http://www.economist.com/blogs/economist-explains/2013/04/economist-explains-how-does-bitcoin-work; http://www.theguardian.com/technology/2011/jun/22/bitcoins-how-do-they-work.

3 This may not seem like a lot, but they are divisible and tradeable down to 8 decimal places. See http://bitcoin.org/en/about.

4 The original paper can be found at http://bitcoin.org/bitcoin.pdf.

5 Bitcoins were worth so little that at some point in May 2010, someone used 25,000 bitcoins to purchase a pizza. This would later prove to be a poor investment, as at the current value of a bitcoin, this pizza cost $3 million.

6 http://motherboard.vice.com/blog/who-is-satoshi-nakamoto-the-creator-of-bitcoin

(or the Winklevii), the former Olympic rower entrepreneurs made famous by their involvement in the foundation of Facebook (and subsequent legal battle). The Winklevii invested heavily in Bitcoin, and in July of 2013 they announced plans to create a Bitcoin fund.[7]

Finally, the value of Bitcoin began to increase – at first steadily and then far more rapidly. At the beginning of 2013, a bitcoin was worth roughly USD $15. However, across 2013, Bitcoin has faced a roller-coaster ride, with a bitcoin peaking at over $250, falling to $70, and then recovering to $160, before falling and rising again. At the time of writing, a bitcoin was available for exchange for $120 USD.[8]

How Bitcoin and the law interact going into the future may partly depend on the continued pace and uptake of them as a form of currency, as well as the ability for governments to develop the technical capacity to trace and monitor them

Bitcoin and the Regulators

The question remains as to how Bitcoin will be dealt with by the law. The concerns surrounding potential money laundering and other financial crimes using Bitcoin has not gone unnoticed by the regulators.

The approach taken in relation to Bitcoin by the central bank of Thailand to date has been relatively straightforward. On 31 July, Thai Bitcoin exchanges suspended trading after the central bank declared that trading in Bitcoins, or using them to buy or sell goods, was illegal. The central bank stated that, due to lack of existing laws to deal with the virtual currency, and its nebulous place in the financial industry, they were outside of applicable existing laws and therefore illegal.[9] This approach was a tacit admission by Thai authorities of the difficulties existing laws were having grappling with this new concept of virtual currency.

In the US, more nuanced approaches have been taken. The first sign that Bitcoin was being taken seriously by law enforcement authorities was when US Treasury issued a guidance note in March of this year which clarified that the financial crimes regulations will also apply to "virtual currencies".[10] These rules were specifically designed to capture products such as Bitcoin and included references to trading in "e-currencies or e-precious metals". The regulations are aimed at monitoring "administrators" or "exchangers" of virtual currencies, targeting Bitcoin exchange organisations as potential areas of money laundering.

Bitcoin exchanges have been subject to several subpoenas, with some having accounts frozen by US regulators.[11] In July, Mt Gox, the largest Bitcoin exchange, registered with the US Treasury Financial Crimes Enforcement Network as an official currency exchange for the purpose of US regulation.[12]

In Australia, while there has been little formal action to regulate Bitcoin, the Australian Taxation Office recently indicated that it was monitoring the currency, and that it considered that it could still be subject to taxation in a similar manner to any other currency, including GST or income tax.[13]

Bitcoin and the Courts

The position of regulators in Australia and the US appears to be that Bitcoin is money or a financial product capable of coming under their oversight, whereas Thailand has taken the opposite view. The choice between these two views was exactly what was put before a judge in the recent US Federal Court case of *Security Exchange Commission v Trendon T Shavers and Bitcoin Savings and Trust*.[14]

In this case, handed down on 6 August 2013, the defendant (a self-proclaimed online "pirate") owned and operated Bitcoin Savings and Trust (formerly known as First Pirate Savings and Trust), an investment scheme which had lost large amounts of money through Bitcoin-related investment. The US Security Exchange Commission (***SEC***) accused the pirate, Mr Shavers, of running a Ponzi scheme in breach of US federal *Securities Act 1993* and *Exchange Act 1934*. Mr Shavers, in a daring move, countered that the court had no jurisdiction to hear the matter.

Mr Shavers argument was that investments in the Bitcoin Savings and Trust were not securities because, simply, Bitcoin was not money, and not anything regulated by US law. Since all transactions were in Bitcoin, no money ever changed hands. In response, the SEC argued that these investments were both investment contracts and notes for the purpose of US security legislation.[15]

Judge Mazzant briefly described the nature of Bitcoin in his judgment, noting that it is "an electronic form of currency unbacked by any real asset and without specie, such as coin or precious metal". He described its peer to peer system of users validating transactions, outside of central banking or government authority.

Under US securities legislation, a "security" includes an "investment contract". An "investment contract" involves, among other elements, an "investment of money". The question to consider was whether Bitcoin was "money". Judge Mazaant responded as follows:

> *It is clear that Bitcoin can be used as money. It can be used to purchase goods or services, and as Shavers stated, used to pay for individual living expenses. The only limitation of Bitcoin is that it is limited to those places that accept it as currency. However, it can also be exchanged for conventional currencies, such as the U.S dollar, Euro, Yen and Yuan. Therefore, Bitcoin is currency or a form of money, and investors wishing to invest in BTCST provided an investment of money.*[16]

Given this decision, it was held that the court did have subject matter jurisdiction. The case against Mr Shavers and his piratical ambitions will continue.

---

7 "Winklevoss twins launch Bitcoin fund", The Guardian, 3 July 2013, accessible from: http://www.theguardian.com/technology/2013/jul/02/winklevoss-twins-launch-bitcoin-fund.

8 Bitcoin Charts, accessible from: http://bitcoincharts.com/

9 Trotman, A. "Bitcoins banned in Thailand", *The Telegraph*, 29 July 2013, accessible from: http://www.telegraph.co.uk/finance/currency/10210022/Bitcoins-banned-in-Thailand.html.

10 See FIN-2013-G001, Guidance: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, 18 March 2013, accessible from http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.

11 Toor, A. "US seizes and freezes funds at biggest Bitcoin exchange", *The Verge*, 15 May 2013, accessible from: http://www.theverge.com/2013/5/15/4332698/dwolla-payments-mtgox-halted-by-homeland-security-seizure-warrant/in/3709249.

12 Kastrenakes, J. "Bitcoin trader Mt. Gox registers as currency exchange to comply with US money laundering laws", *The Verge*, 1 July 2013, accessible from: http://www.theverge.com/2013/7/1/4483266/mt-gox-fincen-registration-us-regulation-following-account-seizure.

13 "ATO targets Bitcoin users", *Financial Review*, 24 June 2013, accessible from: http://www.afr.com/p/technology/ato_targets_bitcoin_users_oawpzLQHDz2vEUWtvYLTWI.

14 *SEC v Shavers*

15 ***SEC v Shavers***, p 2-3

16 *SEC v Shavers*, p 3

Conclusion

The place of Bitcoin in the world of financial products and currencies remains uncertain. It is associated with libertarian ideals, of commerce and the digital age. Mr Shavers' argument goes to the core of what Bitcoin considers itself to be – a medium of exchange free from the yoke of government authority, operating in a free and unfettered digital world. However, it is also contradictory to any attempts to legitimise it as a form of alternative currency. The more mainstream Bitcoin becomes, the harder it will be to live up to its promises about freedom, becoming just another form of financial product that is capable of being regulated and (most importantly) taxed.

Staying in the shadows will not help either, as governments will not continue to tolerate a mechanism used largely for illegal means. Recently, bitcoins were seized from a Silk Road drug dealer by US law enforcement.[17] How Bitcoin and the law interact going into the future may partly depend on the continued pace and uptake of them as a form of currency, as well as the ability for governments to develop the technical capacity to trace and monitor them.

The formative years of Bitcoin have been interesting and their relationship with the law will continue to develop. At least for now, Bitcoin is money. How useful it will be as money going forward remains to be seen.

David Rountree is a lawyer at Allens. The views expressed in this article are personal to the author and do not represent any organisation.

17 Biggs, J. "The DEA Seized Bitcoins In A Silk Road Drug Raid", *Techcrunch*, 27 June 2013, accessible from: http://techcrunch.com/2013/06/27/the-dea-seized-bitcoins-in-a-silk-road-drug-raid/.

Postscript:

On 2 October, the FBI and other US regulators shut down the Silk Road website, arrested its alleged founder and seized approximately 26,000 bitcoin (worth around 3.6 million) belonging to Silk Road customers (footnote 1). This is the largest ever seizure of Bitcoin. The issue at play is concerned with the illegal activities of the website, not the use of bitcoins themselves. However, bitcoin prices suffered a dramatic dip in the immediate aftermath (though no more dramatic than any other price change in Bitcoin's history) (footnote 2). This prosecution and investigation by US regulators will play an important part in determining whether Bitcoin goes takes a path hand in hand with, or away from, the illicit activities of the Silk Road, and will be an important phase in the future of digital currencies.

Footnote 1: http://www.theguardian.com/technology/2013/oct/02/bitcoin-silk-road-how-to-seize

Footnote 2: http://www.theguardian.com/technology/2013/oct/03/bitcoin-price-silk-road-ulbricht-value

Thank you to all who celebrated the 25th anniversary of the Communications and Media Law Association (CAMLA) and the CAMLA Cup at Doltone House in August

It was a wonderful evening incorporating the ever popular and always fun CAMLA Cup trivia night hosted by dynamo Debra Richards. We thank Debra and the organising committee – Anita Cade, Cath Hill, Marlia Saunders and Gulley Shimeld and to the staff at Doltone House who took good care of us.

Bruce Meagher, Director of Corporate Affairs at Foxtel delivered a highly entertaining state of the nation address and CAMLA President, Caroline Lovell presented lifetime memberships to CAMLA legends:

- Mark Armstrong (CAMLA founder)
- Victoria Rubensohn (Former CAMLA President)
- Ros Gonczi (Former CAMLA Administrative Secretary)

Congratulations to the CAMLA Cup winner: McCullough Robertson's "TelMacs" team!

A special mention goes out to Deanne Weir for taking out two 'Who am I' questions.

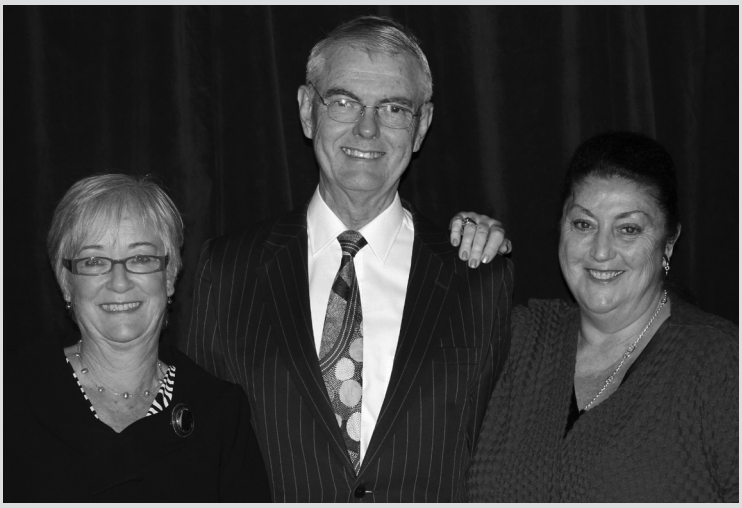
A photo gallery of the evening can be viewed on the CAMLA website www.camla.org.au.

Thank you to Louisa Vickers from Beyond International who kindly stepped in to take some excellent shots for us.

The annual CAMLA Cup could not be possible without the support of our prize donors. CAMLA would like to thank the following firms and organisations for their generous contribution:

Allens
Ashurst
Ausfilm
Baker & McKenzie
Channel Nine
Clayton Utz
Corrs Chambers Westgarth
Discovery Channel
Fox Sports
Foxtel
Gilbert + Tobin
Henry Davis York
International Institute of Communications, Australia
McCullough Robertson
Norton Rose Fulbright
SBS Subscription Channels, Studio and World Movies
Seven Network
Turner Broadcasting
Truman Hoyle
University of New South Wales
Webb Henderson
Yahoo!7

We hope to see you again next year and here's to the next 25 years of CAMLA!



L to R: CAMLA lifetime members: Ros Gonczi, Mark Armstrong and Victoria Rubensohn

Protecting Consumer Data is in Everyone's Interests

Xavier Fijac considers consumer and private sector interests in the use of Big Data.

As the involvement of private sector technology companies in the US government's surveillance program continues to be revealed, Australian consumers may have legitimate concerns about who is accessing their personal and confidential business information. Indeed, the business models of technology giants such as Google, Microsoft, Apple and Facebook and the digital presence of many businesses increasingly rely on access to consumers' personal data. The potential for targeted marketing and the myriad other business applications of Big Data potentially make consumer information the modern day 'rivers of gold'[1]. However consumers have a legitimate expectation that businesses will deal ethically with the information they hand over in exchange for services. Consumer concerns over unexpected or unauthorized use of personal data by the state or the private sector therefore potentially has the power to impede innovation and enterprise in the future digital economy. By acting to maintain the trust of the consumer, the commercial sector may protect the mutual interests of big data and the consumer, and thereby ensure that the rivers of data keep flowing.

The potential for targeted marketing and the myriad other business applications of Big Data potentially make consumer information the modern day 'rivers of gold'

There is little doubt that companies such as Google, Apple, Facebook and Microsoft are deeply engaged in a data economy. That economy is based on the exchange of consumers' personal data for products and services and includes social media platforms, business tools and cloud-based email, search and other communications products. However, the Orwellian flipside of this innovation around a seemingly insatiable appetite for more and more data raises what Bruce Schneier recently referred to as the spectre of a 'public private surveillance partnership'.[2]

This 'partnership' refers to the apparent co-operation of large commercial private enterprises with the requests by government security agencies in the US to hand over vast amounts of consumer data obtained under individual privacy agreements. Governments, so the theory goes, find it convenient to allow this corporate enterprise to expand with minimal regulation. Partly it is said, to encourage enterprise and innovation but also as a convenient defacto mode of collection and storage of ever more data on citizen-consumers, which it would otherwise lack the political will to collect directly. Under the guise of national security, the US government, in this case, simply demands or unilaterally obtains unfettered access, at will.[3] Between private technology and government security, the consumer citizen's interests in the privacy and security of their personal information appear to be largely ignored.

For Australian users of cloud-based services such as Google's Gmail or Apple's iCloud the fact that the servers are located in the US means they may be subject to domestic surveillance in that jurisdiction under the provisions of the Foreign Intelligence Surveillance Act (***FISA***) and the Patriot Act[4]. Additionally, there is some evidence of disclosures by Australian companies of Australian consumers' information to US government agencies, which presumably falls within r the national security exceptions in the Privacy Act 1988 (Cth) (the ***Act***).[5] Here it is worth considering whether the average consumer using a cloud-based product such as Gmail or iCloud would consider it a more serious breach of privacy for that information to be shared between corporations in the private sector, who may in fact already have that information by consent, or to be subject of large-scale government initiated disclosures and exposed to the risk of abuse by low-level officers of domestic foreign government security agencies.[6]

The policy of the former Australian government appeared inconsistent on these points. It is also difficult to predict how genuine the new federal government will be about protecting individual privacy.

On the one hand recent major privacy reforms (which the then Opposition agreed to pass) may place a rather heavy burden on the private sector to manage personal information and come into effect in March 2014.[7] The incoming changes to the Privacy Principles make Australian companies directly liable for the actions of offshore business affiliates to whom they have disclosed information whether knowingly or otherwise, and give the Privacy Commissioner substantial power to impose penalties of up to $1.7 million for serious breaches. On the other hand, the depth and breadth of surveillance demonstrated by revelations about the US National Security Agency (***NSA***) suggests a kind of government surveillance that threatens to undermine the thrust of privacy legislation in Australia on a fundamental level. And at the same time the staff and resources available to the Privacy Commissioner appear so limited we may question how serious the government is about making sure

1 Jim Manamara, "As the 'rivers of gold' dry up, what business model will save media?" The Conversation, 29 June, 2012, http://theconversation.com/as-the-rivers-of-gold-dry-up-what-business-model-will-save-media-7956.

2 Bruce Schneier, 'The Public Private Surveillance Partnership' Bloomberg, July 31, 2013, http://www.bloomberg.com/news/print/2013-07-31/the-public-private-surveillance-partnership.html.

3 Glenn Greenwald, 'NSA PRISM Program taps into user data of Apple, Google and others', June 7, 2013, The Guardian, http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

4 *Foreign Intelligence Surveillance Act of 1978; Uniting And Strengthening America By Providing Appropriate Tools Required To Intercept And Obstruct Terrorism (USA Patriot Act) Act Of 2001*

5 Linton Besser, 'Telstra Storing data on behalf of US Government', July 16, 2013, Sydney Morning Herald, http://smh.com.au/it-pro/security-it/telstra-storing-data-on-behalf-of-us-government-20130716-hv0w4.html

6 http://blogs.wsj.com/washwire/2013/08/23/nsa-officers-sometimes-spy-on-love-interests/

7 *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth); *Privacy Act 1988* (Cth).

the revised Privacy Principles are given force.[8] In this context it seems as though only the open market drivers of consumer behavior (that is, sending their data elsewhere or even refusing to disclose it altogether) may be an increasingly relevant force in shaping the privacy landscape of the future.

Recent developments in the US suggest that technology companies recognize that the impact of consumer behaviour. A recent report by the Washington D.C based think tank 'The Information Technology and Innovation Foundation' suggests that the revelations of the uses of FISA and the Patriot Act could have a real impact on the competitiveness of US based cloud computing industry. The report estimates that the US currently has a 71% market share of what is projected to be a US $200 billion dollar industry by 2016.[9] The threat of a sudden backlash by consumers and businesses concerned about the security of their data stored in US based cloud-systems seems to already be a reality, with 50% of survey respondents in one study indicating an intention to do business elsewhere, and a 45% increase in business for a Swiss hosting company following the PRISM leaks.[10]

The threat of a sudden backlash by consumers and businesses concerned about the security of their data stored in US based cloud-systems seems to already be a reality

The actions of the email company Lavabit LLC, also illustrates emerging ethical concerns around maintaining the confidence of consumers. Lavabit LLC recently announced it would shut down its entire operation, built-up over 10 years and servicing some 400,000 customers, and move to file court proceedings. It was protesting against what it claimed were unreasonable requests from the NSA to disclose personal data of its users, one of whom was Edward Snowden.[11] Although only a single, and no doubt extreme example, the words of the Lavabit founder may be of some concern to the US market more broadly when he said 'this experience has taught me – don't trust private data to a company with physical ties to the USA'.[12]

The largest players in the corporate technology sector are also showing clear signs of discomfort in being seen to form too close a relationship with government at the expense of the consumer. For example, Microsoft's recent advertising campaign 'Your Privacy is Our Priority' is clearly aimed at addressing consumer confidence head on and attempting to gain market share by appealing to user concerns over privacy.[13]

Furthermore, Yahoo CEO Marissa Mayer and Facebook CEO Mark Zuckerberg have recently stepped up the rhetoric in a campaign to increase transparency around NSA information requests to their companies. Both have publicly criticized what they claim are heavy-handed tactics by security agencies such as the threat of treason for non-compliance by business leaders with their disclosure requests.[14] And both Google and Microsoft recently initiated proceedings in US courts challenging the restrictions on their ability to disclose information about the extent of their compliance with government security and the disclosure of consumer data under FISA.[15] This flurry of very public activity seems to be aimed squarely at maintaining consumer confidence for individual users as well as the business community who may already be using their US cloud-based services anywhere in the world.

Australian consumers are operating in a globally connected and cross-border digital economy. This raises complex challenges for data security and maintaining consumer confidence about who has access to their data. Although there are complex multijurisdictional issues raised by off-shore cloud storage and government and corporate access and control of data stored in cloud systems, it appears that the response of large private sector players is crucial to the future of data security and privacy. Companies who identify and respond to the need to protect their reputation by pro-actively addressing these interests are clearly less likely to suffer the potentially damaging financial and reputational consequences of a consumer backlash. Acting to protect consumer privacy concerns therefore stands to be of ethical and commercial benefit to all and may ensure that consumer data, the modern day 'rivers of gold', will continue to flow in the future.

Xavier Fijac is a law student at the University of New South Wales.

---

8 Peter G Leonard 'Lost in the Privacy Landscape' 06 August, 2013, CIO, http://www.cio.com.au/article/522929/lost_privacy_landscape/

9 Daniel Castro 'How Much Will PRISM Cost the US Cloud Computing Industry?' The Information Technology & Innovation Foundation, August 2013, 1.

10 Ibid, 4.

11 Ladar Levison, Owner of Lavabit LLC, statement available at: http://lavabit.com/.

12 Ibid

13 Frederic Lardinois, 'Microsoft Launches New Online Privacy Awareness Campaign' Tech Crunch, April 22, 2013, http://techcrunch.com/2013/04/22/microsoft-launches-new-online-privacy-awareness-campaign

14 Dominic Rushe, 'Zuckerberg: US government 'blew it' on NSA surveillance – Facebook CEO joins Yahoo's Marissa Mayer in saying the US did 'bad job' of balancing people's privacy and duty to protect', The Guardian, September 12, 2013, http://www.theguardian.com/technology/2013/sep/11/yahoo-ceo-mayer-jail-nsa-surveillance

15 Brad Smith, 'Standing Together for Greater Transparency' Microsoft, 30 Aug, 2013, http://blogs.technet.com/b/microsoft_on_the_issues/archive/2013/08/30/standing-together-for-greater-transparency.aspx: Juha Saarinen 'Microsoft, Google sue US govt over spying disclosure', IT News, Aug 21, 2013

What Does the Abbott Government Mean for Online Gambling?

Jessica Azzi considers what the recent Federal election may mean for businesses in the online gambling industry.

Introduction

The Abbott Government has not made any public announcements relating to online gambling. However, the Coalition released two campaign policies during its election campaign, the Helping Problem Gamblers Policy (***Gambling Policy***) and the Policy to Enhance Online Safety for Children (***Online Safety Policy***) (collectively, the ***Policies***), which may be a sign of what the Government has in store not just for the online gambling industry, but for any brand involved in the development or supply of gaming content, including social games.

The Gambling Policy suggests that the Coalition will adopt a conservative approach to online gambling reform. This means that the Government may be unlikely to support existing proposals to amend the Interactive Gambling Act 2001 (Cth) (***IGA***), including the proposals to liberalise online poker and to remove the existing prohibition on online in-play betting.

the Coalition's position that it will not support the future liberalisation of online gambling lowers any expectations in respect of the liberalisation of online in-play betting and online poker

The adoption of this approach is inconsistent with regulatory approaches in a number of countries and would result in the current regulatory framework being maintained. Various parties have suggested that the current framework does not strike the correct balance between:

- the provision of a regulated and competitive Australian online gambling market to Australian residents (which would eliminate the incentive for Australian gamblers to gamble with offshore operators. Extreme difficulties exist in enforcing prohibitions in Australian law, including consumer law prohibitions and gambling law prohibitions, against those operators);
- implementing measures to address problem gambling and harm minimisation which are based on research; and
- in the context of wagering, integrity concerns.

Any framework which is more prohibitive than the one currently in place would be even more removed from this balance.

Background

The IGA prohibits the provision and promotion of "interactive gambling services" (see below) to Australian residents. Both online betting[1] and lotteries are exempt from this prohibition, however, online in-play betting, that is, betting on the outcome of an event after that event has commenced, is not included in this exemption. Operators are permitted to accept in-play bets over the phone. Similarly, totalisators (for example, the TAB), which have a monopoly on retail betting in each State/Territory, are permitted to accept in-play bets over the Counter.

In the 2011-12 financial year, $5.7 billion in turnover was wagered with corporate bookmakers licensed in the Northern Territory. This includes bets on both sport and racing. These licensees include Sportsbet, Sportingbet, bet365, Unibet, Betstar and TomWaterhouse.com.au. These operators, pursuant to their NT licenses, can only accept bets online or via telephone.[2]

It is unknown how much money Australians spend betting online with offshore wagering operators. However, the industry view is that this figure would be substantial and that a significant proportion of this amount is in respect of in-play bets.

Similarly, figures are not available to indicate how much money Australians spend with offshore providers on other types of online gambling, such as online poker and casino games. However, it has been suggested that around 2200 online gambling service providers offer services to Australians in breach of the IGA.[3]

The Department of Broadband, Communications and the Digital Economy (***DBCDE***), the Commonwealth Department responsible for overseeing the IGA, concluded its review of this legislation in early 2013. Its report was published in March 2013 (***DBCDE Report***) and included a number of recommendations, such as:

- that the IGA be amended in respect of in-play betting services to allow online in-play betting, subject to a blanket ban on all micro-betting. A micro bet is, for example, a bet on the outcome of the next ball in cricket or the next point in tennis; and
- the conduct of a 5 year pilot in respect of the licensing of online poker operators which will enable the provision of online poker tournaments, by these licensed operators, to Australian based consumers.

However, on the same day that the DCBDE Report was released, Senator Stephen Conroy, then the Minister for the DCBDE, announced that the focus of the Commonwealth Government would be on developing and implementing a national standard for harm minimisation and consumer protection that covers all licensed online gambling activities. Further, Senator Conroy announced at the time that the Government of the day would not consider the recommended changes relating to online poker or "in-play" sports wagering until agreement is reached in respect of a nationally consistent approach to harm minimisation.

---

1 Wagering is regulated by State/Territory laws, subject to the prohibition on in-play betting contained in the IGA.

2 We note that both Tom Waterhouse and Alan Eskander (of Betstar) each have a Victorian bookmaking licence in their personal capacity. This licence permits them to take bets on-course in Victoria.

3 DBCDE Report. Page 6.

4 http://www.liberal.org.au/helping-problem-gamblers

Driving Australian gamblers offshore?

The Gambling Policy[4] suggests that the Coalition:

- is concerned about the growth of online gambling and that it will be investigating methods of strengthening the enforcement of the IGA to ensure "Australians are protected from illegal online gambling operators";
- will not be supporting any future liberalisation of online gambling; and
- is concerned about the increasing popularity of sports betting and the increase in gambling advertising.

Based on the above, this Gambling Policy, if adopted by the Abbott Government, is likely to have a restrictive impact on the Australian online gambling sector. In particular, the Coalition's position that it will not support the future liberalisation of online gambling lowers any expectations in respect of the liberalisation of online in-play betting and online poker.

However, this position is at odds with the overseas experience which indicates that blanket prohibitions, such as those contained in the IGA, have been unsuccessful in practice in minimising problem gambling.

Further, commentary surrounding recent match-fixing scandals strongly suggests that Australian licensed betting operators assist in the identification of suspicious betting patterns and will report these patterns to the relevant sport's governing body. On the other hand, offshore operators have limited concern (if any) about the protection of the integrity of Australian sport.

Nevada and New Jersey have recently taken steps to regulate both online poker and wagering. There are reports that California, Hawaii, Illinois, Iowa, Massachusetts, Mississippi, Pennsylvania and Texas may follow. Any approach by the Government to limit or halt the Australian market is likely to be inconsistent with measures taken by other jurisdictions to move away from prohibition and towards providing players and operators with the benefits that a regulated jurisdiction brings.

Beyond online gambling

The Online Safety Policy[5] does not refer expressly to gambling but is likely to be of relevance to the social games sector (or any brand which provides games via social media).

A social game has characteristics including that it is offered and hosted by a social networking platform (eg Facebook) or a social gaming platform (eg Xbox Live), it is available for access through a mobile phone app and it places a heavy emphasis on social interaction (eg a player will be encouraged to invite their Facebook friends to play). Examples of popular social games include Slotomania, Candy Crush Saga and Angry Birds.

To fall within the scope of an "interactive gambling service" under the IGA, the "game" must:

(a) be a game of chance or of mixed chance and skill; and
(b) involve consideration; and
(c) be played for money or anything else of value.

If any one or more of these elements is missing, then the game does not constitute an interactive gambling service and does not fall under the ambit of the IGA's prohibitions.

The vast majority of online social games on social networking platforms such as Facebook are legal in Australia as they do not fall within the IGA's definition of "interactive gambling service". This is because they are played for free and, even if there is an initial purchase, the games do not allow players to receive a prize in the form of money, or in a form that can be exchanged for money or anything else of value. That is, online social games fail to satisfy the second and third requirements of a "gambling service".

However, concern has been expressed about certain online social games feature a casino-style or gambling-like content. For example, over the past few years, Senator Nick Xenophon has taken consistently the stance that online social games constitute gambling and are therefore prohibited by the IGA.[6]

The vast majority of online social games on social networking platforms such as Facebook are legal in Australia as they do not fall within the IGA's definition of "interactive gambling service"

The Online Safety Policy indicates the Coalition's intention to strengthen online safety measures to "protect their children from inappropriate material".[7] These proposed measures include:

- the introduction of internet "adult content filters" that will allow consumers to "opt-in" and turn on these filters on their mobile phone and tablet devices or home based internet, to filter out the "inappropriate material";
- establishing a new Children's e-Safety Commissioner, responsible for monitoring online concerns in respect of children; and
- the introduction of a new complaint system, backed by legislation, aimed at removing "harmful material down fast from "large social media sites"". The Policy indicated that, as part of this new complaints system, the Children's e-Safety Commissioner would have the power to direct material to be taken down from the "large social media sites".

The Online Safety Policy does not clarify the scope of "adult content" or "inappropriate or harmful material," however, these measures, particularly the new complaint system, may apply to the online social games sector insofar as they advertise and offer social games on "large social media sites". If concerns such as those held by Senator Xenophon are adopted by the Government, the Online Safety Policy may have a significant effect on the availability of games through channels as mainstream as Facebook and iTunes.

Conclusion

It will be interesting to see what measures, if any, the Government adopts in respect of online gambling reform and whether these measures are balanced and consistent with regulatory changes taking place internationally.

Additionally, it will be important to monitor measures to ensure that the distinction between online social games and online gaming remains clear and that the online social games sector is not unduly covered, inadvertently or intentionally, by proposed amendments to the IGA and made subject to the strict prohibitions that apply generally to online gambling.

Jessica Azzi is a solicitor at Addisons Lawyers. The author would like to thank Jamie Nettleton (a Partner at Addisons) for his assistance with this article. This article represents the views of the author only and does not represent the interests of any organisation.

5 http://lpaweb-static.s3.amazonaws.com/Coalition%202013%20Election%20Policy%20-%20Enhance%20Online%20Safety%20for%20Children.pdf

6 'Nick Xenophon in Bid to Close Gambling App Loophole', The Australian (online), 13 January 2013 <http://www.theaustralian.com.au/national-affairs/nick-xenophon-in-bid-to-close-gambling-app-loophole/story-fn59niix-1226552960088>

7 Please see the Coalition Policy to Enhance Online Safety for Children at:

http://lpaweb-static.s3.amazonaws.com/Coalition%202013%20Election%20Policy%20-%20Enhance%20Online%20Safety%20for%20Children.pdf

The Impact of Social Media in the Workplace: An Employer's Perspective

Veronica Siow examines the key risks for employers who use social media as part of their recruitment and disciplinary processes.

Introduction

The trend of cases coming before Fair Work Commission indicates that employers (and the law) are increasingly grappling with the impact of social media in their workplace. This article considers employers' use of social media as part of their recruitment and disciplinary processes, and some of the issues that arise with respect to such use.

Assessing prospective employees through the social media filter

Increasingly, employers are using social media to assess their prospective employees. There is currently nothing at law that would prevent employers from accessing publicly available information that may be posted by or about a candidate on social media sites such as Facebook, Twitter or LinkedIn. However, in doing so, employers should be aware that there may be legal risks associated with this practice.

An employee's social media posts that humiliate, degrade or harass a work colleague are likely to be in breach of the employer's anti-bullying, anti-harassment policies

Privacy issues

An employer who collects and stores personal information[1] about candidates who are ultimately unsuccessful in their application for employment with the company should be aware that such information will not be captured by the employee records exemption in the *Privacy Act 1988* (Cth). This means that the employer must comply with the National Privacy Principles (or, when they take effect, the Australian Privacy Principles) regarding its collection, use and storage of an unsuccessful applicant's personal information.

Potential adverse action exposure

Employers who in their recruitment decisions take into account information posted by or about their candidates on social media sites should also consider their potential exposure to adverse action claims.

Under the General Protections provisions of the *Fair Work Act 2009* (Cth), prospective employers will have engaged in adverse action if they refuse to employ a prospective employee for a prohibited reason[2] or for reasons which include a prohibited reason.[3]

Let's take the following scenario. A company refuses to employ an otherwise suitable candidate. The candidate becomes aware that the company had during the application process viewed his or her Facebook wall which has a number of posts by the candidate and the candidate's friends and family. The posts suggest that the candidate has a strong union affiliation or indicate the candidate's sexual preference.

In those circumstances, the candidate could allege that the company had made its decision not to employ him or her because of their union membership[4] or because of their sexual preference[5], both of which are prohibited reasons, and in doing so, had engaged in adverse action. With the reverse onus of proof in the adverse action regime, the usual evidentiary hurdles that the candidate might otherwise have faced in making out such a claim are absent. Instead, to defend the claim successfully, the company would have to prove that its decision not to offer the candidate employment was for reason(s) other than the candidate's union affiliation or sexual preference.

In the recruitment space, therefore, employers who seek out information posted on social media sites about their prospective employees before offering employment should ensure that they do not take into account either attributes that are protected by law that their prospective employees appear to have (at least from their posts) or industrial activities in which their prospective employees might engage that are protected under the *Fair Work Act 2009* (Cth).

Disciplining employees for social media conduct

It is reasonably settled law in Australia that an employee's behaviour outside of working hours can give rise to legal consequences for the employee and their employer if there is a sufficient connection between the conduct alleged and the employment.[6] To the extent that the behaviour is said to be a breach of an express term of the employee's contract of employment, such conduct outside the workplace could nevertheless result in the termination of the employment.[7]

Social media posts about colleagues

An employee's social media posts that humiliate, degrade or harass a work colleague are likely to be in breach of the employer's anti-bullying, anti-harassment policies.

In the Good Guys case[8], the employee (Mr O'Keefe) posted on his Facebook (using his home computer, outside of business hours) the following comment:

---

1 "Personal information" for the purposes of the National Privacy Principles means information or an opinion (including information or an opinion forming part of a database), whether or not true, and whether or not recorded in a material form, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, Privacy Act 1988 (Cth).

2 Prohibited reasons, for the purposes of grounding an adverse action, include discriminating on the basis of an attribute that is protected under anti-discrimination law (such as race, religion, age, gender, family or carer's responsibility) and on the basis of industrial activities.

3 Section 342 of the Fair Work Act 2009 (Cth).

4 Section 346 of the Fair Work Act 2009 (Cth).

5 Section 351 of the Fair Work Act 2009 (Cth).

6 Griffiths v Rose [2011] FCA 30

7 Fitzgerald v Smith T/A Escape Hair Design [2010] FWA 7358 at [51]

8 O'Keefe v William Muir Pty Ltd t/as The Good Guys [2011] FWA 5311

Damien O'Keefe wonders how the f*** work can be so f***g useless and mess up my pay again. C***s are going down tomorrow

[Expletives censored for this publication]

The employee's Facebook privacy setting meant that the post was only available to his Facebook friends. Included among his Facebook friends were several fellow employees. Mr O'Keefe's comments on Facebook came to the attention of management and he was dismissed following an investigation. Mr O'Keefe made a claim for unfair dismissal against his employer.

In dismissing his claim, Fair Work Australia (as it was then called) (***FWA***) said that Mr O'Keefe's comments on Facebook were threatening and offensive, and were in breach of his employer's workplace policies on conduct, sexual harassment and bullying. The fact that the comments were made on Mr O'Keefe's home computer, out of work hours did not, in FWA's view, make any difference to this assessment. Even though his employer was not named in the post, there was a sufficient connection to the employment because his work colleagues could have read the post and it would have been obvious to them that Mr O'Keefe's comments were directed at their fellow colleagues (who were female) in their payroll department.

Social media posts about employer

An employer seeking to discipline employees who vent their feelings on social media about the company or their employment conditions will need to consider whether any damage has been done to their brand by the posts and ensure that their response is proportionate.

In the *Dover-Ray v Real Insurance case*, Ms Dover-Ray, a female sales agent in a call centre of Real Insurance had made allegations of sexual harassment against another employee. The allegations were investigated by the employer and it concluded that the allegations were not substantiated. After being informed of the outcome of the investigation, Ms Dover-Ray blogged her feelings on her MySpace page in a post entitled, 'Corruption', in which she referred to the company's values as *"absolute lies"*. Her posts also included comments such as:

- *"I have just been through an investigation that in the end advanced corruption."*
- *"The investigation sought to ensure that the evidence was tampered with, was controlled and was biased."*
- *"It is corruption at every level."*[9]

Soon after she posted the comments, a fellow employee of Real Insurance brought the blog to the company's attention. Real Insurance asked her to remove the blog but she refused and the comments on the blog remained online for a number of weeks. Ms Dover-Ray was summarily dismissed for misconduct primarily related to both her blog and her failure to comply with the direction to remove the blog. She made an unfair dismissal claim against the company.

In dismissing Ms Dover-Ray's unfair dismissal application, FWA held that although she had not identified her employer by name in her post, there was enough information on her MySpace page to tie her comments to Real Insurance. The fact that her MySpace friends included other employees of Real Insurance, and her blog could be read by others in the workplace, was a sufficient connection to her employment. FWA found that the criticisms of the company were so severe that her summary dismissal was justified.

In Fitzgerald v Smith T/A Escape Hair Design, FWA took the view that the employer had not suffered any damage as a result of the employee's Facebook post which criticised her employer for not providing a Christmas bonus. Although the unfair dismissal claim was upheld, Commissioner Bissett in that case made the following observations:

> *a Facebook posting, while initially undertaken outside working hours, does not stop once work recommences. It remains on Facebook until removed, for anyone with permission to access the site to see…It would be foolish of employees to think they may say as they wish on their Facebook page with total immunity from any consequences.*[10]

An employer seeking to discipline employees who vent their feelings on social media about the company or their employment conditions will need to consider whether any damage has been done to their brand by the posts and ensure that their response is proportionate.

This sentiment was echoed by the Full Bench of the FWA in their 2012 decision in Linfox Australia Pty Ltd v Stutsel[11]. Although the Full Bench in that case did not overturn FWA's decision in the first instance[12] to reinstate the employee, the Full Bench did not agree with Commissioner Roberts' characterisation in the earlier decision that the Facebook posts were in the flavour of a pub or café discussion between a group of friends. Instead the Full Bench expressed the view that:

> *The fact that the conversations were conducted in electronic form and on Facebook gave the comments a different characteristic and a potentially wider circulation than a pub discussion. Even if the comments were only accessible by the 170 Faceboook "friends" of Mr Stutsel, this was a wide audience and one which included employees of the Company.*
>
> *…*
>
> *Further, the nature of Facebook (and other such electronic communication on the internet) means that the comments might easily be forwarded on to others, widening the audience for their publication.*
>
> *…*
>
> *Unlike conversations in a pub or café, the Facebook conversations leave a permanent written record of statements and comments made by the participants, which can be read at any time into the future until they are taken down by the page owner. Employees should therefore exercise considerable care in using social networking sites in making comments or conducting conversations about their managers and fellow employees.*

Other conduct on social media

With the proliferation of social and professional networking sites such as Twitter and LinkedIn, two recent cases serve as a timely reminder to employees of the potential for their conduct on social media sites to impact negatively on their employment.

In *Pedley v IPMS Pty Ltd T/A peckvonhartel*[13], the employee was summarily dismissed following his email to a select group of his LinkedIn connections in which he solicited for work for his private interior design service. Among the LinkedIn connections who received the

9 [2010] FWA 8544 at [49]

10 [2010] FWA 7358 at [52]

11 [2012] FWAFB 7097

12 Stutsel v Linfox Australia Pty Ltd [2011] FWA 8444

13 Bradley Pedley v IPMS Pty Ltd T/A peckvonhartel [2013] FWC 4282

email were clients of his employer. Fair Work Commission (***FWC***) upheld the dismissal, finding that the employee's conduct was in breach of his obligations to his employer.

In Banerji v Bowles[14], the employee, Ms Banerji, applied to the Federal Circuit Court for an injunction to prevent her employer, the Department of Immigration and Citizenship, from terminating her employment. Ms Banerji, who at the time the decision was handed down on 9 August 2013 was employed by the Department as a public affairs officer, alleged that her employer had taken, and was in the course of taking, adverse action against her because of her tweets on her Twitter account, *@LALegale*. Her tweets (which the Court noted were sometimes mocking, sometimes critical) were about, among other matters, the practices and policies of the company that provides security services at Commonwealth immigration detention centres, the immigration policies of the Australian Government and the employees of the Department.

Ms Banerji claimed that the Department was taking adverse action against her by seeking to dismiss her because she had expressed her political opinion. She further claimed that the Department's action was in breach of her constitutional right as a citizen to express a political opinion. Her employer contended that Ms Banerji's comments on her Twitter account were in breach of the Australian Public Service's Code of Conduct and the Department's Guidelines on Use of Social Media by DIAC Employees.

Ms Banerji sought declaratory orders that the Department's finding that she had breached the APS Code of Conduct was a contravention of her implied unfettered constitutional right of political communication. The Court refused to make such orders, finding that no such unfettered right exists. The Court rejected any contention that Ms Banerji's political tweets, while employed by the Department under an employment contract and while subject to the APS Code of Conduct and the Department's social media guidelines, were constitutionally protected.

The Court also denied Ms Banerji's application for an injunction to stay the termination of her employment.

Summing up the employer's response

Employers must act promptly once they become aware of any alleged social media misconduct by an employee, and respond in a manner that:

- observes procedural fairness (by investigating the alleged misconduct and providing the employee with the opportunity to respond to the allegations);
- is proportionate to the misconduct (by ensuring that the disciplinary action to be taken is appropriate to deal with the misconduct, and taking into consideration also whether any damage has been suffered by the employer); and
- is consistent with its past responses to similar misconduct by other employees.

Conclusions

The cases discussed in this article show that while it remains necessary for there to be some connection between the employee's behaviour and the workplace, the prominence of social media in employees' daily life has increased the ways in which the employee's comments outside of work could make it back to their employer and become a workplace issue. To respond to these issues and minimise any adverse impact of such conduct in the workplace, employers should consider having policies on social media, anti-bullying/anti-harassment and technology usage that set out clearly the consequences for employees whose social media conduct breaches company policy or the employees' duties to their employer.

Veronica Siow is a Senior Associate at Allens. The views expressed in this article are personal to the author and do not represent any organisation.

14 [2013] FCCA 1052

Link in with CAMLA

Keep in touch with all things CAMLA via the new Communications and Media Law Association LinkedIn group.

You will find information here on upcoming seminars, relevant industry information and the chance to connect with other CAMLA members.

LinkedIn is the world's largest professional network on the internet with 3 million Australian members.

To join, visit www.linkedin.com and search for "Communications and Media Law Association" or send an email to Cath Hill - camla@tpg.com.au

Contributions & Comments

Contibutions and Comments are sought from the members and non-members of CAMLA, including features, articles, and case notes. Suggestions and comments on the content and format of the Communications Law Bulletin are also welcomed.

Contributions in hard copy and electronic format and comments should be forwarded to the editors of the Communications Law Bulletin at editor@camla.org.au or to

Valeska Bloch or Victoria Wark

C/- Allens
Deutsche Bank Place
Corner Hunter & Philip Streets
SYDNEY NSW 2000

Tel: +612 9230 4000
Fax: +612 9230 5333

CAMLA contact details:

Email: camla@tpg.com.au
Phone: 02 9399 5595
Mail: PO Box 237,
KINGSFORD NSW 2032

Communications & Media Law Association Incorporated

The Communications and Media Law Association (**CAMLA**) brings together a wide range of people interested in law and policy relating to communications and the media. CAMLA includes lawyers, journalists, broadcasters, members of the telecommunications industry, politicians, publishers, academics and public servants.

Issues of interest to CAMLA members include:

- defamation
- broadcasting
- copyright
- advertising
- information technology
- freedom of information
- contempt
- privacy
- censorship
- film law
- telecommunications
- the Internet & on-line services

In order to debate and discuss these issues CAMLA organises a range of seminars and lunches featuring speakers prominent in communications and media law policy.

Speakers have included Ministers, Attorneys-General, members and staff of communications regulatory authorities, senior public servants, executives in the communications industry, lawyers specialising in media and communications law, and overseas experts.

CAMLA provides a useful way to establish informal contacts with other people working in the business of communications and media. It is strongly independent, and includes people with diverse political and professional connections. To join CAMLA, or to subscribe to the Communications Law Bulletin, complete the form below and forward it to CAMLA.

Disclaimer

The Communications Law Bulletin is the journal of the Communications and Media Law Association (**CAMLA**) which is an independent organisation which acts as a forum for debate and discussion and welcomes the widest range of views. The views expressed in the Communications Law Bulletin and at CAMLA functions are personal views of the respective authors or speakers. They are not intended to be relied upon as, or to take the place of, legal advice.

CAMLA Website

Visit the CAMLA website at www.camla.org.au for information about CAMLA, CAMLA seminars and events, competitions and the Communications Law Bulletin.

Application for Membership

To: The Secretary, camla@tpg.com.au or CAMLA, Box 237, KINGSFORD NSW 2032
Phone: 02 9399 5595

Name:.....

Address: .....

Telephone: .....Fax: .....Email: .....

Principal areas of interest: .....

.....

I hereby apply for the category of membership ticked below, which includes a Communications Law Bulletin subscription, and enclose a cheque in favour of CAMLA for the annual fee indicated:

☐ I Ordinary membership $130.00 (includes GST)

☐ Student membership $45.00 (includes GST)
(please provide photocopy of student card - fulltime undergraduate students only)

☐ Corporate membership $525.00 (includes GST)
(list names of individuals, maximum of 5)

☐ Subscription without membership $150.00 (includes GST)
(library subscribers may obtain extra copies for $10.00 each + GST and handling)