Hacking By Australian Journos? A Risky Proposition

Nick Sinclair considers how existing laws in Australia would apply to electronic hacking by the local media.

Introduction

For much of July, the now defunct *News of the World* (***NOTW***) was just that. The revelations leading to the closure of the 168-year-old London tabloid reverberated around the globe, and were pursued with particular zeal in Australia, not least by those who favour an overhaul of privacy laws.

The events in the United Kingdom have prompted questions about the practices of Australian media outlets and their reporters.[1] Amongst some in the political class, these questions have led to calls for government inquiries into media regulation, including media ownership.[2] Among lawyers (including the Minister for Justice, Brendan O'Connor), the NOTW saga has triggered a fresh round of debate about the merits of a tort of invasion of privacy.[3] Although no such cause of action is currently available in any Australian jurisdiction, either under statute or at common law, a 2008 Australian Law Reform Commission report[4] which recommended statutory recognition of a cause of action for serious invasions of privacy is now being dusted off and reconsidered.

Notwithstanding the potential merits of such a reform (particularly as it might relate to unintentional conduct by large organisations in the course of handling of personal data), there has been little analysis of existing laws in Australia and how they might apply if Fleet Street hacking techniques were ever deployed in this country. This article explores the existing sanctions and remedies that would apply to electronic hacking conducted by or on behalf of media outlets in Australia. Despite the media exemption in the *Privacy Act 1988* (Cth),[5] Australian reporters are not immune from prosecution for intentionally intercepting or accessing private communications. This article also proposes a modest amendment to State and Territory criminal codes, which would better safeguard electronic files stored on a computer.

Telecommunications

The *Telecommunications (Interception and Access) Act 1979* (Cth) (the ***Interception and Access Act***) broadly prohibits the interception of communications,[6] except where authorised in special circumstances.[7]

Section 7 of the Interception and Access Act deals with communications 'passing over a telecommunications system', where 'passing over' is defined to cover communications that are in transmission.[8] Section 7 would apply to sophisticated methods of electronic interception to listen in on telephone calls in real time and/or record them for subsequent replay.

> ***there has been little analysis of existing laws in Australia and how they might apply if Fleet Street hacking techniques were ever deployed in this country***

The methods used in the NOTW saga were far more rudimentary. Essentially, they were designed to take advantage of security weaknesses around stored voice mail messages. The techniques described as 'hacking' often consisted of nothing more than obtaining the target individual's mobile phone number, dialling a general voice mail retrieval service and entering a default PIN code in the hope that the target had not already adopted a new PIN.[9]

The unauthorised access of a target's voicemail messages is not caught by section 7 of the Interception and Access Act because like SMS messages and email, a voicemail, for the purposes of the Interception and Access Act, stops passing over a telecommunications system when 'it becomes accessible to the intended recipient of the communication'.[10] Nonetheless, in 2006 the federal government amended the Interception and Access Act,[11] making it an offence to access 'stored communications' (including SMS, email and voicemail) without the knowledge of the sender or the intended recipient of the stored communication.

Section 108 of the Interception and Access Act, which makes the unauthorised access of stored communications an offence, stipulates that the penalty for breach can include up to two years' imprisonment.[12] Of particular interest to editors, publishers and others who

---

1 To date, there have been no serious suggestions, let alone evidence, of phone hacking (or similar conduct) by employees or contractors of any Australian media outlet.

2 See, eg, Shane McLeod, "Bob Brown pushes for media inquiry" (14 July 2011), ABC News <http://www.abc.net.au/news/2011-07-14/bob-brown-calls-for-media-review/2794992> at 6 September 2011.

3 On 21 July 2011, the Minister for Justice cited the NOTW scandal in announcing that the Gillard Government would issue a public issues paper "canvassing the prospect of introducing a statutory cause of action for serious invasions of privacy": "A right to privacy in Australia", Minister for Home Affairs/Minister for Justice/Minister for Privacy and Freedom of Information (21 July 2011) <http://www.ministerhomeaffairs.gov.au/www/ministers/oconnor.nsf/Page/MediaReleases_2011_ThirdQuarter_21July2011-ArighttoprivacyinAustralia> at 6 September 2011.

4 Australian Law Reform Commission, *"For Your Information: Australian Privacy Law and Practice"*, Report 108 (12 August 2008).

5 *Privacy Act 1988* (Cth), s7B(4).

6 *Telecommunications (Interception and Access) Act 1979* (Cth) s7.

7 These include law enforcement and certain acts done by employees of carriers in the course of their duties.

8 *Telecommunications (Interception and Access) Act 1979* (Cth) s5F. "Communications" is defined to include "conversation and a message, and any part of a conversation or message", whether in the form of: (i) speech, music or other sounds; (ii) data; (iii) text; (iv) visual images, or (v) signals, "in any form or in any combination of forms". A "telecommunications system" is a telecommunications network within Australia (or partly within Australia), including equipment, a line or other facility connected to such network.

9 Default PIN codes are usually '1234' or '0000'.

10 *Telecommunications (Interception and Access) Act 1979* (Cth) s5F.

11 Via the *Telecommunications (Interception) Amendment Act 2006* (Cth)

12 In respect of live communications, under s105 it is an indictable offence (punishable by up to 2 years imprisonment) to contravene s7 by intercepting communications that are passing over a telecommunications system.

the NOTW saga has triggered a fresh round of debate about the merits of a tort of invasion of privacy.

manage journalists is the provision in section 108 of the Interception and Access Act that extends the offence to a person who 'authorises, suffers or permits' another to access stored communications, and to anyone who 'does any act or thing' that enables them or another to gain access.[13]

Supplementing these criminal sanctions are the civil remedies in the Interception and Access Act,[14] which empower both civil and criminal courts to grant remedial relief to an 'aggrieved person' whose communications (including stored communications) are accessed in breach of the Interception and Access Act. Section 165, which sets out the civil remedies for the unlawful access of stored communications, includes a non-exhaustive list of orders that a court can make. These include an order for damages (specifically including punitive damages),[15] injunctive relief and an order to pay the aggrieved person 'total gross income derived by the defendant as a result of the access or communication, as the case requires'.[16] A plaintiff can obtain the benefit of these civil remedies in relation to both the unlawful access of communications and the subsequent communication of information obtained from such access.[17]

These civil remedies allied with possible criminal sanctions make for a particularly robust legislative framework, which would likely apply if NOTW's methods were replicated in Australia. Especially significant, in the event of interception of private communications by a media organisation, is the possibility of an order to pay an aggrieved person an amount equivalent to the income earned by the defendant from accessing the communication (in addition to general and punitive damages).

A harsher range of consequences for anyone found to have illegally intercepted communications or accessed stored messages is difficult to imagine. For Australian media organisations, the Interception and Access Act should act therefore as a powerful deterrent of the type of behaviour that brought down NOTW.

Computer Hacking

Rudimentary as NOTW's techniques were, it is easy to imagine a modern-day reporter trying their hand (or at least engaging someone else in the task) at something more sophisticated than simply hacking into voicemail message banks. The application of the provisions of the Interception and Access Act detailed above to computer hacking would depend primarily on whether the accessed information was contained in a stored communication or was passing over a telecommunications system (in, for example, an email).

In many if not most instances of computer hacking, it is likely that the Interception and Access Act would apply, given that communications passing over the internet, and those stored on an internet service provider's equipment, fall within its ambit.

But what about a simple Word or PDF document, saved on an individual's hard drive but never transmitted over a telecommunications system or stored on an ISP's equipment, which is somehow hacked into and accessed by a reporter (or anyone else for that matter)? In most parts of Australia, this kind of hacking would be unregulated. The computer offences contained in the Commonwealth Criminal Code[18] do not prohibit access per se. The same is true in the equivalent state legislation in New South Wales, Victoria, the Australian Capital Territory and South Australia.[19] As the Australian Institute of Criminology has explained, '[i]n this scheme there has been a deliberate choice to peg criminal liability at four levels based on the defendant's intent or the way access to data is secured on a computer'.[20] In other words, under the Criminal Code and the equivalent State laws, a computer offence is not committed unless the act of hacking is accompanied by some other intent or motivation (for example, the intent to commit some other serious offence against a law of the Commonwealth, or of a State or Territory, by the access, modification or impairment of the computer in question).[21]

As illustrated by the example of a hacked Word or PDF document, there appears to be a gap in the law in Australia, at least outside of the Northern Territory.[22]

Section 276B of the *Criminal Code Act* (NT) is unique in Australia. It prohibits the unlawful access of data held in a computer with intent to 'gain benefit or advantage, whether personally or for a third party'.[23] This provision would likely apply to computer hacking

The application of the provisions of the Interception and Access Act detailed above to computer hacking would depend primarily on whether the accessed information was contained in a stored communication or was passing over a telecommunications system (in, for example, an email)

13 *Telecommunications (Interception and Access) Act 1979* (Cth) s108(1)(a)(ii) and (iii).

14 *Telecommunications (Interception and Access) Act 1979* (Cth) ss107A and 165.

15 *Telecommunications (Interception and Access) Act 1979* (Cth) s165(10).

16 *Telecommunications (Interception and Access) Act 1979* (Cth) s165(7)(d).

17 Section 165 of the Interception and Access Act also provides for remedial relief where a person breaches s133 by communicating information obtained from the unlawful accessing of a stored communication.

18 *Criminal Code Act 1995* (Cth), Schedule – The Criminal Code, Part 10.7.

19 Each of these States has implemented a series of computer offences broadly similar to those added to the Commonwealth Criminal Code by the *Cybercrime Act 2001* (Cth): see *Crimes Act 1900* (NSW) Part 6; *Crimes Act 1958* (Vic) Part 1, Division 3, Subdivision 6; *Criminal Law Consolidation Act 1935* (SA) Part 4A; *Criminal Code 2002* (ACT) Part 4.2.

20 'High tech crime brief no. 5: Hacking offences', Australian Institute of Criminology (January 2005) <http://www.aic.gov.au/en/publications/current%20series/htcb/1-20/htcb005.aspx> at 6 September 2011.

21 *Criminal Code Act 1995* (Cth), Schedule – The Criminal Code, s477.1(1)(d).

22 This is not to say that other remedies would not available under Australian law, depending on the circumstances in which the document was accessed. A victim in such a case might be able to prevent dissemination of the information in the document through an action grounded in unconscionability or the equitable doctrine of breach of confidence. The tort of trespass could also be an option in certain circumstances.

23 *Criminal Code Act* (NT), s276B(1).

under the Criminal Code and the equivalent State laws, a computer offence is not committed unless the act of hacking is accompanied by some other intent or motivation

by a journalist seeking private information, even if it fell outside the ambit of the Interception and Access Act.[24] The prescribed penalty in the NT is up to 10 years' imprisonment.

A move by the other States and Territories to adopt the NT's position on computer offences would be a modest reform in the face of fresh concerns about electronic hacking.[25] Given the small gap that currently exists in Australia vis-à-vis electronic privacy invasions by media, this may be a wiser course of action than holding out for a wide-ranging new tort of privacy.

Conclusion

Despite the possible merits of a comprehensive new tort of invasion of privacy, either statutory or at common law, Australian legislators and judges have been reluctant to pursue it. The reluctance may be explained by the limited constitutional protection of free speech in Australia. Not only does the existing range of laws provide a number of sanctions, remedies and safeguards (particularly against the sort of conduct canvassed in this article), but the concept of privacy is both fluid and nebulous, and not necessarily amenable to broad-brush legal reform.[26]

Australia is not out of step with other common law countries; indeed it seems there are almost as many legal approaches to privacy as there are jurisdictions. Since the *European Convention on Human Rights* was implemented in the UK by way of the *Human Rights Act 1998* (UK), British courts have certainly become more willing to award damages for invasion of privacy, albeit by broadening the equitable action for breach of confidence rather than recognising a new tort.[27] After years of competing judgments on the issue in the Canadian province of Ontario, a judge of the Superior Court recently held that 'there is no tort of invasion of privacy in Ontario'.[28] Although Ontario, like Australia, does not have a statutory tort (unlike several other common law provinces in Canada),[29] Whitaker J noted in *Jones v Tsige* that 'it cannot be said that there is a legal vacuum that permits wrongs to go unrighted – requiring judicial intervention'.[30] The case, which had no media connection, involved the access by a bank employee of a colleague's private financial records stored on a workplace computer, the plaintiff also being a customer of the bank in question (interestingly, if an Australian reporter accessed similar electronically-stored information, the case may fall into the legal gap identified above). The court squarely rejected the plaintiff's assertion that she would be without a remedy in the absence of a tort of invasion of privacy.[31]

US courts recognise four distinct strands of an invasion of privacy tort.[32] However, members of the High Court of Australia commented on US privacy law in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* as follows:

> *'Privacy law in the United States delivers far less than it promises, because it resolves virtually all these conflicts in favour of information, candour, and free speech. The sweeping language of [US] privacy law serves largely to mask the fact that the law provides almost no protection against privacy-invading disclosures.'*[33]

A minor tweak to existing statutes could adequately cover a small gap in the law that applies to electronic invasions, which in any event is already robust and potentially quite severe

Rather than reacting to the NOTW story in a manner that risks constraining local journalists – who are not shielded by protections such as those contained in the US Constitution – and possibly compromising free speech, proponents of Australian privacy law reform may wish to carefully consider the existing legal framework. A minor tweak to existing statutes could adequately cover a small gap in the law that applies to electronic invasions, which in any event is already robust and potentially quite severe.

Nick Sinclair is a lawyer in the Technology, Media and Telecommunications Practice Group at Allens Arthur Robinson.

---

24 Queensland (*Criminal Code 1899*, s408E), Western Australia (*Criminal Code Act Compilation Act 1913*, s440A) and Tasmania (*Criminal Code Act 1924*, Chapt XXVIIIA) each have unique computer offences unlike those in the NT and the other States and Territory. But none of the respective offences in those States would be as likely to apply to a journalist who hacked into private computer files which were not stored communications as the offence in the NT. Section 257D of Tasmania's *Criminal Code Act 1924*, which prohibits any computer hacking "without lawful excuse", is the most robust; but the lack of a definition for "without lawful excuse" creates uncertainty.

25 The Commonwealth would arguably be precluded from adopting such an amendment to its own Criminal Code, given that its Constitutional authority in relation to creating criminal offences is limited.

26 In extracurial remarks seven years after the High Court's decision in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, Chief Justice Gleeson remarked that "[t]he ground seems to me to be shifting under the concept of privacy... I wrote a judgment a few years ago in which I said there seemed to me to be certain things that were self-evidently private. I'm not so sure about that any more. When you look at the kind of information that people publish about themselves it makes you wonder": Nicola Berkovic, "Why Privacy isn't what it used to be," (22 August 2008) *The Australian* <http://www.theaustralian.com.au/business/legal-affairs/why-privacy-isnt-what-it-used-to-be/story-e6frg97x-1111117263398> at 6 September 2011.

27 Australian Law Reform Commission, *"For Your Information: Australian Privacy Law and Practice"*, Report 108 (12 August 2008) at 74.27-74.28.

28 *Jones v Tsige* 2011 ONSC 1475 at [57].

29 Including British Columbia, Saskatchewan, Manitoba and Newfoundland & Labrador: see Australian Law Reform Commission, *"For Your Information: Australian Privacy Law and Practice"*, Report 108 (12 August 2008) at 74.23.

30 *Jones v Tsige* 2011 ONSC 1475 at [53].

31 The judge suggested an alternative cause of action could have been found in Canada's *Personal Information Protection and Electronic Documents Act 2000*, which applies to the banking sector.

32 'Intrusion Upon Seclusion', 'Appropriation of Name or Likeness', 'Publicity Given to Private Life' and 'Placing a Person in False Light': *Restatement of the Law, 2nd, Torts, 1977* (US).

33 (2001) 208 CLR 199 at [119].