LexisNexis

# Privacy Law Bulletin

2019 . Vol 16 No 8

## Contents





*Information contained in this newsletter is current as at November 2019*

LexisNexis Butterworths

Privacy Law
Bulletin

# Contracting for the disclosure of personal information between organisations: lessons from the Shahin decision

***Helen Clarke, Viva Swords*** *and* ***Sarah Clouston*** *CORRS CHAMBERS WESTGARTH*

## Key takeaways

- There are a number of lessons in *Shahin Enterprises Pty Ltd v BP Australia Pty Ltd*[1] (*Shahin*) to ensure that multi-entity direct marketing activities are privacy-compliant.
- Entities must comply with Australian Privacy Principle (APP) 7 (direct marketing), not APP 6 (use or disclosure of personal information), in relation to the disclosure of personal information for the purposes of the recipient undertaking direct marketing.
- If an obligation to provide personal information is expressed to be "subject to privacy laws", then the obligation to provide that information may be defeated if the discloser has not put in place the relevant requirements to ensure that the information can be shared in compliance with privacy laws.

## Introduction

There are obvious privacy risks associated with the disclosure of personal information by one organisation to another. When drafting a contract for such an arrangement, the privacy risks and implications should be handled comprehensively and sensitively. The judgment by Blue J in *Shahin* demonstrates that an insufficient attention to detail and the privacy regulatory regime may thwart such an arrangement.

## The factual background of the Shahin decision

While the decision in *Shahin* discusses a number of different claims by the applicants, this article will focus on the claim in relation to the contractual requirement to disclose personal information.

On 26 September 2013, Shahin and BP entered into an agreement under which BP supplied branding rights and fuel for certain Shahin-operated service stations in South Australia (Agreement). Clause SC21 provided that, subject to relevant privacy legislation, BP must regularly provide to Shahin information reasonably requested about BP cardholders who visit Shahin's service stations, so that Shahin could market goods and services to those customers. In this article, this type of disclosure is referred to as a "business to business disclosure".

The reference to "BP card customers" is a reference to those customers with a "BP Plus" card, which could be used by a cardholder to purchase fuel at BP-branded service stations. Customers applying for a BP Plus card agree to be bound by the Terms and Conditions of use of the BP Plus card attached to the application (Cardholder Terms).

On 23 August 2016, Shahin made a request for BP cardholder information under cl SC21 of the Agreement. BP refused that request on the basis that it could not disclose that information to Shahin in compliance with the Privacy Act 1988 (Cth).

Among other claims, Shahin alleged that BP had breached the Agreement by failing to provide BP cardholder information in accordance with cl SC21 of the Agreement. This claim was unsuccessful; Blue J ultimately concluded that BP could not disclose that information to Shahin in compliance with the Privacy Act, so the condition of cl SC21 was not fulfilled. However, in the course of coming to this conclusion, his Honour conducted a detailed analysis of APPs 6 and 7 and was not shy about criticising the drafting of them. He also commented on some of the most fundamental concepts underpinning the Privacy Act, including consent, reasonable expectation and the primary purpose of collection.

## Lesson 1: Don't make an obligation conditional if you don't want it to be thwarted by the condition failing.

This case provides an important reminder that contracting parties should carefully consider any conditions imposed on contractual obligations when negotiating

and administering contracts. Blue J considered that the qualifying words "subject to relevant privacy legislation" mean that BP is not obliged to provide Shahin with customers' personal information in compliance with cl SC21 if doing so, or any use by Shahin of that information for direct marketing, would breach the Privacy Act.

Parties should ensure that, where they make an obligation conditional on compliance with the Privacy Act, they are aware of the restrictions of the Privacy Act and how it might affect — or, in this case, thwart — the obligation.

## Lesson 2: APP 7, not APP 6, applies where there is business to business disclosure for the purposes of direct marketing. Where the information is not sensitive information, the relevant exception that might allow the disclosure is in APP 7.3.

### *Which APP applies?*

BP contended that, while APP 7 addresses use or disclosure by an organisation for the purposes of direct marketing by that organisation (primary organisation), it does not address disclosure by an organisation for the purpose of direct marketing by another organisation (secondary organisation). BP submitted instead that APP 6 addresses this situation.

It is here that Blue J's critique of the APP drafting came into play. His Honour expressed the view that the draftsperson "[had] not adequately grappled with the various dichotomies"[2] within APP 7 and between APPs 6 and 7, including issues that would arise where there is business to business disclosure for the purpose of direct marketing by the secondary organisation. While this ambiguity in the APPs rendered BP's submission "arguable", Blue J ultimately rejected it and held that APP 7 applied to the situation at hand. Interestingly, the judge appeared to be of the opinion that neither APP 6 nor APP 7 is well-adapted to deal with the disclosure in question.

### *Which exception in APP 7 applies?*

That decision did not mark the end of Blue J's woes with APP 7, as his Honour next had to determine whether the exceptions in APP 7.2 and 7.3 (relating to the use of personal information other than sensitive information for direct marketing purposes, subject to certain conditions) applied.

Again appearing dissatisfied with the drafting of the APPs, Blue J came to the conclusion that the exception in APP 7.2 is not available to parties looking to allow business to business disclosure for personal information other than sensitive information; rather, parties must rely solely on APP 7.3.

In doing so, his Honour noted that some conditions of APP 7.3 can only be satisfied by the organisation that actually undertakes the direct marketing (ie, the secondary organisation). Those conditions of APP 7.3 are inapplicable to business to business disclosures. However, the secondary organisation itself will be prohibited from using the information received for direct marketing unless it satisfies those conditions.

The analysis in the judgment to come to this finding about the applicable APP was rigorous. However, it produces the curious result that if the secondary organisation never actually goes on to use the personal information for direct marketing, then APP 7 applied to the disclosure between the primary organisation and the secondary organisation, even though no direct marketing was actually undertaken.

## Lesson 3: A privacy policy is not a contract.

The Cardholder Terms stated that BP's collection, storage, disclosure and use of the customer's information would be performed in accordance with BP's Privacy Policy. Shahin argued that this drafting incorporated the Privacy Policy into the Cardholder Terms and consequently authorised disclosure by BP of the personal information to its dealers for the purpose of direct marketing by them.

Blue J held that this drafting does not incorporate the provisions of the Privacy Policy into the Cardholder Terms. Rather, it merely directs the customer's attention to provisions of the Privacy Policy. His Honour stated that this construction is reinforced by the fact that the Privacy Policy is a statement of BP's policy around personal information rather than an agreement between BP and individuals whose personal information may be collected.

Contracting parties should therefore ensure that any relevant privacy obligations are included in the contract itself, rather than relying on a reference to comply with a privacy policy.

## Lesson 4: Just because a list of purposes for which personal information is used is non-exhaustive, does not mean that the purposes are unlimited.

The Cardholder Terms contain an acknowledgment by the customer that BP may use the customer's personal information for "additional purposes including" three purposes explicitly listed in the clause. Shahin argued that this acknowledgment embodied a consent by customers to BP using the personal information for any additional purpose whatsoever without any limitation. In particular, Shahin pointed to a general interpretation clause in the Cardholder Terms which stated that "including" means "including without limitations".

First considering the acknowledgment in the absence of the interpretation clause, Blue J held that the reference to "additional purposes including" would not mean that BP can use the information for any purpose whatsoever. Rather, it designates that BP could use the information for purposes incidental to the primary purposes of assessing the customer's application for a card and administering the account, and for the three identified additional purposes identified in the acknowledgment. Context was significant here — it is extremely unlikely that the customer intended to consent to BP using the information for any purpose whatsoever.

Blue J then highlighted that general interpretation clauses yield when the context of a specific usage indicates otherwise. The stipulation that "including" means "including without limitations" therefore did not change his Honour's decision.

Parties who want to use personal information for additional purposes would be well advised to explicitly list those purposes or ensure that they are incidental to the primary purpose.

## Lesson 5: There can be more than one "primary purpose" of collection under APP 6 … but there usually won't be many.

Blue J also provided useful guidance on the interpretation of APP 6. BP submitted that, if APP 6 (rather than APP 7) applied to the disclosure of information by a primary organisation to a secondary organisation for the purpose of direct marketing by the latter, the drafting of APP 6.1 only contemplates and permits a single primary use. BP's argument hinged on the fact that APP 6.1 refers to information collected for "a" particular purpose, which is then defined to be "the" particular purpose.

Blue J rejected this interpretation, noting that, as a matter of construction, use of the singular is often understood to encompass the plural. He did, however, state that the purposes for which information is collected will "necessarily be finite" and will generally be of a very limited number if more than one.

## Lesson 6: The case as to an implied term has still not been judicially considered, but could be available.

Shahin contended that, if BP was not required by cl SC21 to provide Shahin with the personal information, BP had an implied obligation to amend the Cardholder Terms in such a manner as would avoid it being a breach of the Privacy Act for BP to disclose the information to Shahin or Shahin to use the information for direct marketing. Shahin argued that this obligation arose from the implied duty by parties to cooperate and do all that is necessary for carrying out the agreed matters to ensure the other party receives the intended contractual benefits (as articulated by the House of Lords in *Mackay v Dick*.[3]

Unfortunately for those seeking clarification on the validity of this argument, Blue J held that Shahin did not properly plead its case. His Honour stated that the implied duty of cooperation requires cooperation by both parties. Before BP could be said to be in breach of any such obligation, it would be necessary for Shahin to formulate proposed amendments to the Cardholder Terms and for BP to refuse or fail to make the amendments in circumstances where it is required to do so.

Despite Blue J's rejection of Shahin's argument in this case, His Honour's reasoning indicates that, in a similar case where the argument is properly pleaded, it may be open for a judge to hold that there is an implied term.

## Where to from here?

Blue J ended his judgment with an unequivocal call for the APPs to be redrafted in light of the ambiguities highlighted in the *Shahin* decision. Is anyone listening? In March 2019, the Australian Government announced a raft of initial changes to the Privacy Act and indicated that an exposure draft of legislation would be available later in 2019. Perhaps through that process the draftsperson will revisit APPs 6 and 7 to address the criticism in *Shahin*.

In the meantime, *Shahin* will be one of the most authoritative decisions on the aspects of the Privacy Act that it considers, until such time as a later case is decided or superseding guidance from the Office of the Australian Information Commissioner is published.

***Helen Clarke***
*Partner*
*Corrs Chambers Westgarth*
*helen.clarke@corrs.com.au*
*https://corrs.com.au/*

***Viva Swords***
*Associate*
*Corrs Chambers Westgarth*
*viva.swords@corrs.com.au*
*https://corrs.com.au/*

***Sarah Clouston***
*Lawyer*
*Corrs Chambers Westgarth*
*sarah.clouston@corrs.com.au*
*https://corrs.com.au/*

## Footnotes

1. *Shahin Enterprises Pty Ltd v BP Australia Pty Ltd* [2019] SASC 12; BC201900597.
2. Above, at [129].
3. *Mackay v Dick* (1881) 6 App Cas 251.

Privacy Law
Bulletin

# Carer vetting: identity data sharing under the National Disability Insurance regime

***Dr Bruce Baer Arnold*** *UNIVERSITY OF CANBERRA*

What do we know about people who are employed to care for disabled peers under the National Disability Insurance Scheme (NDIS), the much-criticised social support scheme?[1] New legislation to underpin that scheme should allay some fears about abuse by care workers but involves questions about the sharing of personal information. As with other large-scale intergovernmental data sharing mechanisms there is an assumption that data provided locally but accessible nationally will be accurate, with low accountability and lower remedies if something goes wrong.

The National Disability Insurance Scheme Amendment (Worker Screening Database) Act 2019 (Cth) (2019 Act) establishes a cooperative database for nationally consistent disability worker screening. The expectation is that the legislation, which amends the National Disability Insurance Scheme Act 2013 (Cth) (2013 Act) and is to be reflected in state/territory law, will minimise "the risk of harm to people with disability from those who work closely with them."[2] The database will be co-funded by the Commonwealth, states and territories. It will enable wide access to a range of information about many Australians and thus has a significant privacy aspect. It is bounded by Ch 4 of the 2013 Act that features provisions regarding the collection, use and disclosure of the NDIS vetting information.

Salient aspects for practitioners advising employers, workers and third parties such as government agencies and rights advocates are:

- the legislation provides for a centralised database administered by the NDIS Quality and Safeguards Commissioner, drawing on personal information from all Australian jurisdictions
- the database centres on decisions regarding exclusion, suspension, revocation or authorisation of activity as a worker under the NDIS but includes a range of personal identifiers
- information in the database will be shared with a large number of public and private sector entities rather than merely the Commissioner and Commonwealth Department of Social Services
- as with several identity databases, there is scope for extension through ministerial directive
- there are potential concerns with the accuracy of information transferred to the database

## Basis

The Commonwealth does not have an exclusive head of power regarding vetting of workers as a facet of the NDIS, which instead has a cooperative basis. The Act reflects the February 2017 agreement by the Council of Australian Governments regarding the Intergovernmental Agreement on Nationally Consistent Worker Screening for the NDIS and the Disability Reform Council National Disability Insurance Scheme Quality and Safeguarding Framework. The Agreement and Framework encompass a "nationally recognised approach to worker screening". The states and territories are responsible for conducting NDIS worker screening checks, including the application process (including criminal history checks) and risk assessment, with a new database being hosted by the NDIS Quality and Safeguards Commission (QSC) for its Commissioner.

The 2013 Act currently provides for the screening of workers of registered NDIS providers.[3] The National Disability Insurance Scheme (Practice Standards—Worker Screening) Rules 2018 (Cth) provide for worker screening requirements as part of the NDIS Practice Standards.[4] Compliance with those Standards is a condition of registration, with the Rules requiring that workers engaged in certain work must have a clearance under a state or territory NDIS worker screening statute.[5]

The 2019 amendment provides for the Commonwealth Minister to make a non-delegable determination, via legislative instrument, that a law of a state or territory is a "NDIS worker screening law" for the purposes of the definition of that term in s 9 of the 2013 Act. Under a new s 10B, state/territory laws establishing a scheme for worker screening in relation to the NDIS can be specified for the database as they are made or amended by each jurisdiction. A law will only be an NDIS worker screening law once it has been specified in a determination by the Minister under s 10B.

Section 10B(1) provides that a legislative instrument made under the new section is not subject to disallowance by way of the Legislation Act 2003 (Cth).[6] For a determination under new s 10B, the Minister must have the agreement of the state/territory that has enacted the law being specified.

## Coverage

The Explanatory Memorandum states that the database:

> ... is intended to be a centralised repository of information about persons who have had decisions made about them, or who have applied to have decisions made about them, under NDIS worker screening law. It is intended to be current and up to date, reflecting an accurate picture of whether a person, in working or seeking to work with people with disability, does or does not pose a risk to such people.[7]

The database will thus hold personal information about people who have applied for an NDIS worker screening check, alongside any pending, current and previous decisions made by the state/territory screening unit in relation to that application — a capacious category given the number of people engaged in the NDIS sector and the sort of information that might be considered by units in screening those people. Screening may of course creep beyond the NDIS to other sectors, as noted below. Employers, including self-managed participants, will have scope to require worker screening for any person that they engage in the delivery of NDIS services.

Importantly, the Explanatory Memorandum states that the Commission:

> ... will work with State and Territory governments to put in place a nationally consistent, risk-based decision-making framework for considering a person's criminal history and patterns of behaviour over time to guard against the unreasonable exclusion of people who have committed an offence or misconduct from working in the disability sector, where this is not relevant to their potential future risk to people with disability.[8]

Given the above comments information in the database may be shared with a wide range of entities at varying levels of detail. These include state/territory screening units conducting worker screening checks; registered NDIS providers and their subcontractors; the National Disability Insurance Agency and its contractors; entities providing services under Ch 2 of the 2013 Act (in essence on the basis of funding under the NDIS); unregistered NDIS providers and their subcontractors; self-managed participants and plan nominees; the NDIS QSC; and the Department of Social Services. Sharing may be extended through addition of an additional purpose of the database determined in an instrument under s 181Y(8).

What information might be included? The database may contain information about an individual who has applied for a screening check and information relating to that application, including personal information about the applicant, date of the application and the jurisdiction or territory in which their application was made.[9] It may include information about a person whose application is no longer being considered and the reasons.[10]

Saliently, the database may provide information about someone cleared to work with people with disability and information relating to a decision, under an NDIS worker screening law at any point in time (including who made the decision, the reasons for that decision and the period during which the decision remains in force).[11] The corollary is inclusion of information about a person who is prevented from working with people with disability, including who made the decision and the reasons for that decision.[12]

The database may feature information about any interim decision made while an application is still being considered (for example, restriction on working with people with disability while their application is pending). It is anticipated that a new decision (including another interim decision) may replace the initial interim decision once the application is determined. For comprehensiveness that the database covers, people whose clearance to work with people with disability has been suspended or revoked.[13]

The legislation does not set the level of detail of the reasons noted above and the Explanatory Memorandum thus states:

> The database will not contain information about a person's criminal history, including convictions and charges and any other information relied on to support a decision that is made under NDIS worker screening law. It will also not contain information about a person's sexual identity or preferences.[14]

Section 181Y(6) indicates that the range of information that may be featured on the database is intended to be broad but is limited to information necessary for the performance of the Commissioner's function in establishing and maintaining the database, and the purposes of the database as outlined in s 181Y(3), alongside limits on the Commissioner's information collection, use and disclosure powers under the 2013 Act.

The database will however encompass a range of personal information, including sensitive information relating to disability status, Aboriginal and Torres Strait Islander status and cultural and linguistic diversity status. That information may thus feature an individual's name, date of birth, age, place of birth, address, telephone number, email address, other contact details,

employment details, education, government-issued identification numbers and expiry dates as well as a worker screening number allocated to that person.

The database is not restricted to current/potential employees. The 2019 Act provides that the database may contain information about employers or potential employers who may hire persons who have made screening applications, with "employers" encompassing self-managed participants who may hire their own workers.[15] That information includes the person's potential, current and previous employers, including contact details, period of employment, a description of the role the person was employed in and the period of time they were in that role.

## Employer access

The Explanatory Memorandum for the NDIS amendment states:

> ... employers will have access to a limited subset of information on the database. This is expected to include information about a worker's identity, so that an employer can verify that the person who holds the clearance is the same person that they have engaged or intend to engage. Employers will also have access to information related to whether or not a person they have engaged is cleared to work in certain roles. Employers will not have access to the details of a worker's other employers, or sensitive information relating to a worker's disability status, Aboriginal and Torres Strait Islander status or cultural and linguistic diversity status.[16]

From a rights perspective, that restriction is not a major concession, given that employers will presumably collect employment history and sensitive personal data from potential employees in the course of recruitment. That data will be covered by the Privacy Act 1988 (Cth) and state/territory enactments independent of the amended NDIS Act.

Most end users, ie, people receiving support under the NDIS, will remain reliant on data collected and used by third parties such as service providers; the Act does not provide comprehensive information access rights for consumers.

## What is accessible?

As it stands, the legislation provides that the range of information that may be contained on the database is limited to information necessary for the performance of the Commissioner's functions and for the purposes of the database.

Historically, such limitations have tended to creep, whether because of administrative convenience or in response to negative media coverage regarding specific incidents and criticisms by parliamentary committees.

Section 181Y(5)(j) thus enables the Minister to determine additional information to be contained within the database by way of legislative instrument under s 181Y(8). Additional content of the database accordingly might include a new type of decision contemplated by the screening law but not already covered by s 181Y(5), with the expectation that flexibility will facilitate ongoing implementation of state/territory screening laws under the NDIS.

The Explanatory Memorandum states that:

> States and Territories will have full access to the database as required to effectively implement the national policy, including the ongoing monitoring of people who hold clearances, and the identification of fraudulent or duplicate applications, such as where a person has made multiple attempts to gain a worker screening clearance in a different jurisdiction or under a different name.[17]

That statement might be contextualised by reference to the recent NSW Law Enforcement Conduct Commission's (LECC) *The New South Wales Child Protection Register: Operation Tusket Final Report*,[18] which revealed systemic problems with operation of the key sex offender register over more than a decade.

The Commission stated:

> ... there have been problems with the Register for 17 years. Significant errors in the application of the CPOR Act started occurring as early as 2002. These errors have included incorrect decisions by the NSW Police Force about which persons should be included on the Register, and incorrect decisions about how long persons were legally required to make reports of their personal information to police under the CPOR Act (their "reporting period").
>
> Some of these errors have resulted in child sex offenders being in the community without being monitored by the NSW Police Force as required by the CPOR Act. The Commission reviewed one case in which a person reoffended while unmonitored. Other errors have caused the NSW Police Force to unlawfully require people to report their personal information to police for a number of years. As a result, people have been wrongly convicted, and even imprisoned, for failing to comply with CPOR Act reporting obligations, when in fact those obligations did not apply to them at the relevant time. Two persons were unlawfully imprisoned for more than a year in total.
>
> The NSW Police Force has been aware for a number of years that there were significant issues with the Register. In 2014 the NSW Police Force Child Protection Registry (the Registry), the specialist unit in the State Crime Command responsible for maintaining the Register, started filing internal reports warning of systemic issues causing inaccuracies in the Register. Multiple reports from the Registry prompted the NSW Police Force to review 5,749 Register case files. This review was started in 2016 and took two years to complete. In October 2018 it concluded that 44 per cent (2,557) of those Register case files had contained errors.[19]

There has not been a comprehensive cross-jurisdictional report on the accuracy of the offender registers in each of the Australian jurisdictions, but practitioners and policymakers might suspect that the

under-resourcing evident in NSW (reflective of misplaced priorities and budget stringencies) will be present in other locations and result in systemic problems regarding operation of the other offender databases.

## Accountability

Under the national policy for NDIS worker screening, the states and territories will provide review and appeal rights to workers who may be subject to an adverse decision, bearing in mind that:

> ... some individuals, by virtue of their history, have valuable lived experiences to share with people with disability accessing NDIS supports and services. It is recognised that people with lived experience who have committed an offence or misconduct in the past can make significant changes in their lives.[20]

The expectation is that a review of an adverse decision regarding an individual will be consistent with principles of natural justice and procedural fairness. The states/territories will disclose reasons for an intention to make an adverse decision (other than where NDIS screening units are required under Commonwealth, state or territory law to refuse disclosure). Awareness of the intention to make the adverse decision is envisaged as allowing individuals a reasonable opportunity to be heard, with the decision-maker considering the individual's response before finalising the decision.

## Looking ahead

The legislation is restricted to the NDIS. It does not provide for comprehensive registration of or sharing of data about all carers — remunerated or otherwise — in the aged, education or mental health sectors.

Practitioners might however consider whether the legislation provides a model for comprehensive sharing of data on a sector-by-sector basis about the identity of a wide range of people who are employed or gratuitously engage with vulnerable minors and adults, including education (primary, secondary and tertiary) and aged care. The latter sector is likely to be salient given both the shifting demographics of the Australian population — we are, alas, all getting older and more people will require care in future — and current inquiries into abuses in aged care and mental health care.[21]

***Dr Bruce Baer Arnold***
*Assistant Professor*
*Faculty of Law*
*University of Canberra*

## Footnotes

1. M Foster et al "'Reasonable and necessary' care: the challenge of operationalising the NDIS policy principle in allocating disability care in Australia" (2016) 51(1) *Australian Journal of Social Issues* 27; and Productivity Commission *National Disability Insurance Scheme (NDIS) Costs* (October 2017) www.pc.gov.au/inquiries/completed/ndis-costs/report/ndis-costs.pdf.
2. Explanatory Memorandum, National Disability Insurance Scheme Amendment (Worker Screening Database) Bill 2019 https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6269_ems_d6028f13-3eab-4745-837e-f43147ede861/upload_pdf/698368.pdf;fileType=application%2Fpdf at 1.
3. National Disability Insurance Scheme Act 2013, ss 73B, 73E, 73F, 73J and 73T.
4. Above, s 73T.
5. Above n 3, s 73F.
6. Legislation Act, s 44(1).
7. Above n 2, at 4.
8. Above n 2, at 11–12.
9. Above n 3, s 181Y(5)(a).
10. Above n 3, s 181Y(5)(b).
11. Above n 3, s 181Y(5)(c).
12. Above n 3, s 181Y(5)(e).
13. Above n 3, s 181Y(5)(g) and (h).
14. Above n 2, at 7.
15. Above n 3, s 181Y(5)(i).
16. Above n 2, at 13.
17. Above n 2, at 13.
18. LECC *The New South Wales Child Protection Register: Operation Tusket Final Report* (October 2019) www.lecc.nsw.gov.au/news-and-publications/publications/final-version-operation-tusket-report-28-october-2019.pdf.
19. Above, at 16.
20. Above n 2, at 11.
21. Note for example the Commonwealth Royal Commission into Aged Care Quality and Safety, where submissions are highlighting concerns regarding substantive abuses in aged care facilities.

Privacy Law
Bulletin

# Australia's mandatory decryption law

***Peter Leonard*** *DATA SYNERGIES and UNSW BUSINESS SCHOOL, SYDNEY*

## Key points

In 2018, the Attorneys-General of the so-called Five Eyes countries — the USA, the United Kingdom, Canada, Australia and New Zealand — stated concerns that online businesses design their systems in a way that precludes any form of access to content. As stated in a communique following their meeting in London on 30 July 2019:

> This approach puts citizens and society at risk by severely eroding a company's ability to identify and respond to the most harmful illegal content, such as child sexual exploitation and abuse, terrorist and extremist material and foreign adversaries' attempts to undermine democratic values and institutions, as well as law enforcement agencies' ability to investigate serious crime. Tech companies should include mechanisms in the design of their encrypted products and services whereby governments, acting with appropriate legal authority, can obtain access to data in a readable and usable format.[1]

The communique also stated their call for:

> ... detailed engagement between governments, tech companies, and other stakeholders to examine how proposals of this type can be implemented without negatively impacting user safety, while protecting cyber security and user privacy, including the privacy of victims.[2]

Australia and the UK led the way in legislating for a mandatory right of government to require decryption of encrypted communications. The law was passed in December 2018 in the face of concerted opposition from both industry, privacy advocates and civil society organisations. Most unusually, soon after enactment this law is under review. This article reviews the content of, and controversy surrounding, Australia's mandatory decryption law.

## Overview

The Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth) (the Act) came into law in December 2018. This Act amended a range of Commonwealth legislation, to empower law enforcement and national security agencies to request, or compel, assistance from a broad range of telecommunications and online service providers. The Act also established powers which enable law enforcement and intelligence agencies to obtain warrants to access data and devices and amended the search warrant framework under the Crimes Act 1914 (Cth) and the Customs Act 1901 (Cth) to expand the ability of criminal law enforcement agencies to collect evidence from electronic devices.

The Act added a new Pt 15 to the Telecommunications Act 1997 (Cth). This Part applies to providers of telecommunications services within Australia, and providers of encryption products and encryption-based internet services that have one or more end users in Australia. The fact that a provider has its head office in Australia (or elsewhere) is not relevant. A service or product provider becomes subject to a legally enforceable obligation to assist decryption of communications by customers if a technical assistance notice or a technical capability notice is issued in accordance with Pt 15.

A technical assistance notice or technical capability notice must not require a provider to do any act or thing which would require a legal warrant or legal authorisation under relevant statutes. The consequence is intended to be that a technical assistance notice or technical capability notice cannot be used as an alternative to a warrant or authorisation under any relevant statute.

A technical assistance notice or technical capability notice must be reasonable, proportionate, practicable and technically feasible.

A technical assistance notice or technical capability notice must not:

- have the effect of requiring a relevant entity to implement or build a systemic weakness, or a systemic vulnerability (such as, but not only, to implement or build a new decryption capability), into a form of electronic protection (such as authentication and/or encryption)
- prevent a designated communications provider from rectifying a systemic weakness, or a systemic vulnerability, in a form of electronic protection

References to implement or build a systemic weakness, or a systemic vulnerability, into a form of electronic protection include:

- any action that would render systemic methods of authentication or encryption less effective

- any act or thing that will, or is likely to, jeopardise the security of any information held by any other person

"Systemic vulnerability" is defined as a vulnerability that affects a whole class (particular mobile device models, carriage services, electronic services or software) of technology (rather than a single item of technology) but does not include a vulnerability that is selectively introduced, on a case-by-case basis, to one or more target technologies that are connected with a particular person.

Issue of notices are subject to relatively prescriptive and detailed thresholds and other requirements of the Act. There are significant controls and safeguards in the Act. These controls and safeguards are manifestly less than ideal, but they will operate as significant checks upon exercise by Australian agencies of powers conferred by this Act.

The provisions of the Act are not apt to legally compel a provider of a product or service to actively consult with, and work with, a user of a provider's product or service to break or workaround encryption.

## Review

The Act passed the Australian Parliament on 6 December 2018, following extensive amendments that were made to the Bill by the government overnight to secure passage of the Bill late in the evening of the last parliamentary sitting day of the calendar year 2018. These amendments included some amendments to the Bill that the Australian Labor Party had previously proposed as a condition for their support of passage of the Bill. The Opposition agreed to passage of the Bill as "an emergency measure" to address statements by Government Ministers as to an allegedly heightened terrorist threat over the Christmas–New Year period. The then Labor leader called a media conference to announce that support for passage of the Bill was conditioned upon:

- firstly, substantial narrowing of the circumstances in which the new powers could be exercised
- second, inclusion of a range of controls and safeguards and transparency measures
- third, the Bill returning to the Parliamentary Joint Committee for Intelligence and Security (PJCIS) for further scrutiny and consideration

The PJCIS commenced a review[3] of the amendments made by the Act. The Committee is required to report by 13 April 2020. The Committee resolved to focus on the following aspects of the legislation:[4]

- the threshold, scope and proportionality of powers provided for by the Act;
- authorisation processes and decision-making criteria;
- the scope of enforcement provisions and the grant of immunities;
- interaction with intelligence agencies other powers;
- interaction with foreign laws, including the United States' *Clarifying Lawful Overseas Use of Data Act*;
- impact on industry and competitiveness; and
- reporting obligations and oversight measures.

In March 2019, the PJCIS requested that the Independent National Security Legislation Monitor (INSLM) commence a review of operation, effectiveness and implementation of amendments made by the Act, focused upon whether the Act:

- contains appropriate safeguards for protecting the rights of individuals
- remains proportionate to any threat of terrorism or threat to national security, or both
- remains necessary

The INSLM is due to report by 1 March 2020, to enable any findings to then inform the Committee's review.

In parallel with these reviews, the Department of Home Affairs conducted consultations with the telecommunications industry as to proposed guidance on administration of the Act. Following that consultation, the Department issued *Industry assistance under Part 15 of the Telecommunications Act 1997 (Cth): Administrative guidance for agency engagement with designated communications providers*.[5] This document:

> … outlines administrative processes and best-practice for the use of the measures in Part 15. This guidance has been designed for use by both Government stakeholders and members of the communications industry to ensure that all parties have a clear understanding of their rights, obligations and expectations. It should be used by persons interacting with the assistance framework, whether they are within an agency seeking assistance or within a company providing assistance. The guide also sets out the limitations of the regime and establishes the administrative parameters of Part 15.[6]

Meanwhile, similar legislated decryption initiatives are underway in other Five Eyes countries.[7]

## How the current Act operates

The Act does not change the requirement for law enforcement, security and intelligence agencies to obtain a judicial warrant or other lawful authorisation to require an entity holding information about communications to provide particular information about those communications, and to obtain a judicial warrant to provide the content of communications (sometimes referred to as payload data).

The Act adds a power to enable issue of warrants that legally compel a covered entity to assist a limited number of Australian law enforcement, national security

and law enforcement agencies to fulfil an objective of enabling the relevant Australian agency to access encrypted communications of a particular person over a particular service or through a particular product.

The Act also confers lawful authority on an entity that receives a "technical assistance request" to provide assistance to relevant Australian agencies to fulfil an objective of enabling the relevant Australian agency to access encrypted communications of a particular person over a particular service or through a particular product, without infringing other laws or legal restrictions, such as privacy and confidentiality requirements.[8] This memorandum does not deal further with requirements as to technical assistance requests as many organisations will elect not to voluntarily assist relevant Australian agencies to access encrypted communications.

The Act creates two types of lawful authority that relevant Australian law enforcement agencies may obtain to legally compel a particular entity to provide lawful assistance with the objective of enabling the relevant Australian agency to endeavour to access encrypted communications.

## Technical assistance notices and technical capability notices

The two types of legal compulsion are "technical assistance notices" and "technical capability notices", as respectively described below.

These notices may be issued to entities that relevantly include entities that provide services facilitating encrypted communications, and entities that develop, supply or update software used, for use, or likely to be used, in connection with a communications carriage service or an electronic service that has one or more end users in Australia.[9]

These categories of covered entities would include persons involved in designing trust infrastructure used in encrypted communications or software utilised in secure messaging applications.

The categories of covered entities are drafted to require a relevant nexus to Australia. A geographical nexus provision enables Australian agencies to request assistance from offshore entities that have a relevant role in the provision of relevant products or services in Australia, or to and from Australia. For example, the Act will apply to Amazon, AWS, Google, Apple, Facebook (WeChat), Microsoft, Alibaba, Huawei and Tencent.

A relevant notice has no effect to the extent it requires a relevant entity provider to do an act or thing which would require a warrant or authorisation under certain relevant statutes, with the consequence that a relevant notice cannot be used as an alternative to a warrant or authorisation under any of those statutes.[10]

A relevant notice must be reasonable, proportionate, practicable and technically feasible.[11]

A relevant notice must not:

- have the effect of requiring a relevant entity to implement or build a systemic weakness, or a systemic vulnerability (such as, but not only, to implement or build a new decryption capability), into a form of electronic protection (such as authentication and/or encryption)
- prevent a designated communications provider from rectifying a systemic weakness, or a systemic vulnerability, in a form of electronic protection

References in the Act to implement or build a systemic weakness or a systemic vulnerability into a form of electronic protection include:[12]

- one or more actions that would render systemic methods of authentication or encryption less effective
- any act or thing that will, or is likely to, jeopardise the security of any information held by any other person

"Systemic vulnerability" is defined as a vulnerability that affects a whole class (particular mobile device models, carriage services, electronic services or software) of technology (rather than a single item of technology), but does not include a vulnerability that is selectively introduced, on a case-by-case basis, to one or more target technologies that are connected with a particular person.

"Systemic weakness" means a weakness (something that makes general items of technology less secure) that affects a whole class of technology (rather than a single item of technology), but does not include a weakness that is selectively introduced, on a case-by-case basis, to one or more target technologies that are connected with a particular person.[13]

While systemic weaknesses or vulnerabilities cannot be built into services or devices, a notice can require the selective introduction of a weakness or vulnerability into a particular service, device or item or software (the "target technology") that is provided to a particular person, but a notice can only do so on a case-by-case basis.

Both technical assistance notices and technical capability notices must only introduce requirements that are "reasonable and proportionate", having regard to (among other things):[14]

(a) the interests of national security;
(b) the interests of law enforcement;
(c) the legitimate interests of the designated communications provider to whom the notice relates;

(d) the objectives of the notice;
(e) the availability of other means to achieve the objectives of the notice;
(ea) whether the requirements, when compared to other forms of industry assistance ... are the least intrusive form of industry assistance [having regard to interests of persons whose activities are not of interest to [Australian Security Intelligence Organisation] ASIO and whose activities are not of interest to interception agencies];
(eb) whether the requirements are necessary;
(f) the legitimate expectations of the Australian community relating to privacy and cybersecurity[.]

## Key differences between a technical assistance notice and a technical capability notice

Key differences between a technical assistance notice and a technical capability notice include the following.

### *What the notice may require*

A technical assistance notice may require the provider to do acts or things by way of giving certain types of help to ASIO or the agency in relation to:

- enforcing the criminal law, so far as it relates to serious Australian offences[15]
- assisting the enforcement of the criminal laws in force in a foreign country, so far as those laws relate to serious foreign offences, or
- safeguarding national security

A technical capability notice may require the provider to do acts or things directed towards ensuring that the provider is capable of giving certain types of help to ASIO or an interception agency in relation to these matters.

As noted in the Explanatory Memorandum:

> Division 4 allows the Attorney-General to issue a technical capability notice that is directed towards ensuring that the designated communications provider is capable of giving listed help to ASIO or an interception agency. However, a technical capability notice cannot be used to compel a provider to build a capability that would enable it to remove encryption, or any form of electronic protection, from products. The things specified in technical capability notices may require significant investment. The capabilities built under a technical capability notice may be utilised by multiple agencies. This is distinct from assistance required by a technical assistance notice under new section 317L which can oblige a provider to give help that they are already capable of providing to the requesting agency.[16]

In all cases the reasonable costs incurred by the provider in complying with a notice must be reimbursed by the agency issuing the notice.[17]

### *Who may issue the notice?*

A technical assistance notice may only be issued by the Director-General of Security, or the chief officer of an interception agency (the Australian Federal Police (AFP), the Australian Crime Commission or the Police Force of a state or the Northern Territory),[18] in each case with the approval of the AFP Commissioner.[19]

A technical capability notice may only be issued by the Attorney-General, after consultation with the Minister for Home Affairs.[20]

### *Prior consultation requirements*

A provider generally must be consulted before a notice is issued.

In the case of a technical assistance notice, the Director-General of Security or the chief officer of an interception agency, as the case requires, must consult with the provider[21] unless the chief officer of the issuing authority is satisfied that the technical assistance notice should be given as a matter of urgency (in which event there may not be consultation with the provider) or the provider waives compliance with the requirement for consultation.[22]

In the case of a technical capability notice, the Attorney-General must not give a technical capability notice to a provider unless the Attorney-General has:[23]

- given the provider a consultation notice setting out a proposal to give the technical capability
- invited the provider to make a submission to the Attorney-General on the proposed technical capability
- considered any submission that was received within the time limit specified in the consultation notice

A time limit for consultation must run for at least 28 days, unless the Attorney-General is satisfied that the technical capability notice should be given as a matter of urgency or compliance is impracticable (in which event there must still be consultation with the provider, but the consultation period may be foreshortened).[24]

A provider may request carrying out of an assessment by independent assessors (appointed by the Attorney-General):[25]

- one of whom has high security clearance and knowledge that would enable the person to assess whether the proposed technical capability notice would not introduce any systemic weakness or systemic vulnerability and are reasonable, proportionate, practicable and technically feasible (hence not contravening s 317ZG)
- the other being a retired superior court judge

The Attorney-General must consider the report when issuing the notice.[26]

## Confidentiality requirements

The confidentiality requirements of the Act are rigorous and restrictive.

New s 317ZF(1) creates offences where (among others) a provider, an employee, a contracted service provider of a provider or an employee of a contracted service provider of a provider, discloses assessment notice information or technical capability notice information (or information obtained in accordance with a notice.

A person may disclose information:[27]

> (a) in connection with the administration or execution of this Part; or
> (b) for the purposes of any legal proceedings arising out of or otherwise related to this Part or of any report of any such proceedings; or
> (c) in accordance with any requirement imposed by a law of the Commonwealth, a State or a Territory[,]

for the purpose of complying with a technical assistance request, technical assistance notice or technical capability notice.

Disclosure of information relating to relevant notices by providers and their employees is also permitted where the disclosure is authorised in writing by the authority who has given the notice to the provider. Where so authorised (but not otherwise), providers may disclose information about a capability to persons within their supply chain, or where otherwise relevant, with permission of the relevant agency and subject to specified conditions.

## Conclusion

The period for making submissions to the INSLM closed on 1 November 2019. The INSLM will hold public hearings associated with this inquiry in February 2020.

This is an international debate. On 29 October 2019, WhatsApp and Facebook filed a complaint[28] in a federal US court against NSO Group, an international technology company that is alleged to have provided assistance to US authorities in reading encrypted communications sent over WhatsApp. NSO Group is accused of breaches of US state and federal laws, including the US Computer Fraud and Abuse Act. The complaint alleges that NSO Group exploited a vulnerability in WhatsApp's video-calling feature, by sending a user what appeared to be a video call. This was not a normal call: "after the phone rang, the attacker secretly transmitted malicious code in an effort to infect the victim's phone with spyware. The person did not even have to answer the call."[29] This so-called spyware enabled bypass of the WhatsApp enabled encryption of communications over WhatsApp using the "infected" mobile phone. The "attack" "targeted at least 100 human-rights defenders, journalists and other members of civil society across the world." Will Cathcart, the head of WhatsApp (which is owned by Facebook), said:

> Democracies depend on strong independent journalism and civil society, and intentionally weakening security puts these institutions at risk. And we all want to protect our personal information and private conversations. That's why we will continue to oppose calls from governments to weaken end-to-end encryption.[30]

Will Cathcart continued:

> At WhatsApp, we believe people have a fundamental right to privacy and that no one else should have access to your private conversations, not even us. Mobile phones provide us with great utility, but turned against us they can reveal our locations and our private messages, and record sensitive conversations we have with others.[31]

As the continuing debate indicates, there appears no real prospect that the controversy surrounding the Act will abate. The global tech companies remain strongly opposed to mandatory decryption powers. Civil society organisations argue that the policy rationale for mandatory decryption exchanges marginal gains in limited investigative situations for significant loses with regards to individuals' abilities to exercise rights and freedoms through private communications. Financial institutions and other businesses using strong encryption express concerns that mandatory encryption may undermine cybersecurity. Governments point to the most harmful illegal content, such as child sexual exploitation and abuse, and terrorist and extremist material, and argue that they need broad powers in order to detect and address such serious crimes.

Given the continuing concerns of the Five Eyes governments, it appears unlikely that the Commonwealth Act will be repealed. However, the INSLM may be expected to make recommendations to improve controls and safeguards and oversight mechanisms in the Act. None of the stakeholders in this debate will be fully satisfied.

***Peter Leonard***
*Principal, Data Synergies*
*Professor of Practice, IT Systems and Management and Business Law, UNSW Business School*

***About the author***
*Peter Leonard is a Sydney, Australia-based data, content and technology business consultant and lawyer, advising data-driven businesses and government agencies through consultancy Data Synergies. Peter is also a Professor of Practice at UNSW Business School (IT Systems and Management, and Business and Taxation Law). Peter chairs the IoTAA's Data Access, Use and Privacy work stream, the Law Society of New South Wales' Privacy and Data Committee and the Australian Computer Society's AI Ethics Technical Committee. He serves on a number of corporate and advisory boards, including of the NSW Data Analytics Centre. Peter was a founding partner of Gilbert + Tobin.*

## Footnotes

1. UK Attorney General's Office, Joint meeting of Five Country Ministerial and quintet of Attorneys-General: communiqué, London 2019 (Joint meeting), www.gov.uk/government/publications/five-country-ministerial-communique/joint-meeting-of-five-country-ministerial-and-quintet-of-attorneys-general-communique-london-2019; see also the 2018 Communique: Australian Government, Statement of principles on access to evidence and encryption, https://web.archive.org/web/20180925154820/www.homeaffairs.gov.au/about/national-security/five-country-ministerial-2018/access-evidence-encryption.
2. Above.
3. Australian Government, Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/AmendmentsTOLAAct2018.
4. See the Terms of Reference of the review in above n 3, available at www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/AmendmentsTOLAAct2018/Terms_of_Reference.
5. Department of Home Affairs *Industry assistance under Part 15 of the Telecommunications Act 1997 (Cth): Administrative guidance for agency engagement with designated communications providers* (August 2019) www.homeaffairs.gov.au/nat-security/files/assistance-access-administrative-guidance.pdf.
6. Above, at 1.
7. See Joint meeting, above n 1; Canadian House of Commons Standing Committee on Public Safety and National Security *Cybersecurity in the Financial Sector as a National Security Issue* (June 2019) www.ourcommons.ca/Content/Committee/421/SECU/Reports/RP10589448/securp38/securp38-e.pdf; L Gill, T Israel and C Parsons, Shining a light on the encryption debate: a Canadian field guide, 14 May 2018, https://citizenlab.ca/wp-content/uploads/2018/05/Shining-A-Light-Encryption-CitLab-CIPPIC.pdf.
8. See the Explanatory Memorandum and the Supplementary Explanatory Memorandum to the Act, each available at www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6195.
9. Telecommunications and Other Legislation Amendment (Assistance and Access) Act, ss 317C, 317D and 317E.
10. Above, s 317ZH.
11. Above n 9, ss 317J and 317ZAA.
12. Above n 9, s 317ZG.
13. Above n 9, s 317ZG.
14. Above n 9, s 317RA.
15. Serious offence is an offence against a relevant law that is punishable by a maximum term of imprisonment of 3 years or more or for life.
16. Explanatory Memorandum, above n 8, para 142.
17. Above n 9, s 317ZK.
18. Above n 9, ss 317L and 317LA.
19. Above n 9, s 317LA.
20. Above n 9, s 317T.
21. Above n 9, s 317PA.
22. Above n 9, s 317PA(1), (2) and (3).
23. Above n 9, s 317W(1).
24. Above n 9, s 317W(2) and (3).
25. Above n 9, s 317WA.
26. Above n 9, s 317WA(11).
27. Above n 9, s 317ZF(3).
28. See copy of the complaint available at www.washingtonpost.com/context/read-the-whatsapp-complaint-against-nso-group/abc0fb24-8090-447f-8493-1e05b2fc1156/; see also W Cathcart "Why WhatsApp is pushing back on NSO Group hacking" *The Washington Post* 30 October 2019 www.washingtonpost.com/opinions/2019/10/29/why-whatsapp-is-pushing-back-nso-group-hacking/.
29. Cathcart, above.
30. Cathcart, above n 28.
31. Cathcart, above n 28.

# The elephant in the room — is there a tort of invasion of privacy in Australian law? Smethurst v Cmr of Police

***Patrick Gunning*** *KING & WOOD MALLESONS*

Because data is intangible and not protected by a single legal doctrine the law struggles to fashion appropriate remedies when data has been copied or "stolen" in an unauthorised manner. The High Court of Australia faced this issue in a hearing on 12[1] and 13 November[2] 2019 involving a challenge to the validity of a search warrant. Australian Federal Police officers served the warrant on a journalist and required the journalist to enter the passcode to her smartphone, searched the contents of that phone and copied, onto a portable storage device owned by the police, various files that the officers considered were relevant to the alleged criminal offence under investigation. The journalist claimed that the warrant was invalid, and that the copied data should be destroyed. This led to the court wondering whether the journalist was asking the court to recognise a tort of invasion of privacy in Australian law.

Privacy practitioners will be aware that in 2001 the High Court of Australia left open the possibility of the recognition of a tort of invasion of privacy in *Australian Broadcasting Corp v Lenah Game Meats*.[3] Since then, there have been multiple recommendations from federal and state law reform bodies proposing the introduction of a statutory tort, but no Australian government has accepted those recommendations. Nor has any superior Australian court decided whether such a tort is recognised in Australian law.

The court's decision in this case is unlikely to be published until 2020. Privacy practitioners should follow developments to learn if the High Court considers that a tort of invasion of privacy is available in Australian law. For the reasons discussed below, despite the exploration of the question during oral argument, this case is probably not the one that will answer this question.

## Some facts and the debate between the bench and the journalist's counsel

The journalist who challenged the warrant was Annika Smethurst, an employee of Nationwide News Ltd. The search warrant was served on Ms Smethurst[4] in June 2019 at her Canberra home. The police were investigating an alleged leak of information relevant to national security. The case has attracted plenty of media coverage.

This article does not consider the grounds on which the warrant was argued to be invalid. Rather, it focuses on the basis on which the court could grant relief if the warrant was invalid.

The parties had agreed a limited set of facts by way of a "special case", which were considered sufficient to enable the High Court to consider the questions of law said to arise.[5] There had been no trial before a lower court, and no other facts were available. There was no evidence about the contents of the files copied by police officers from the journalist. No doubt a significant reason for this state of affairs would have been caution on the part of the journalist's legal team to not admit a fact that would expose their client to criminal liability if their challenge to the warrant failed.

The journalist's argument was that the invalidity of the warrant meant that the search of her house and personal property was a trespass (a form of tort) — so much is uncontroversial.[6] The next step was to say that the court has power to grant an injunction to reverse the consequences of the trespass. At this point, the bench started to ask some difficult questions of the journalist's counsel, Stephen Lloyd SC:

> KIEFEL CJ: As you say, though, if they had simply taken the information you may have had delivery up for [destruction] under notions like confidential information in equity. But that is not this case.
> MR LLOYD: No, no. But we would say that if they had just taken — if they had seized something we could have asked for it to be returned and an injunction to return it would have undone the tort - - -
> EDELMAN J: But that is easy because if they had seized something you would still have a greater right to possession than the AFP who have taken it.
> NETTLE J: It could be an action in detinue if they have taken documents.
> MR LLOYD: Certainly. So what we say here, to undo the [un]lawfulness that was done during the trespass, or in the course of the trespass, it is a matter of deleting, if the - - -
> EDELMAN J: So your point is that the copying was an unlawfulness - the act of copying was unlawful.

MR LLOYD: It was part of the unlawfulness during the trespass. It was done in effect by force of the warrant. My learned junior is pointing out to me there are two matters. One is the trespass to the property, but the other is the trespass to or conversion of the goods, and using the phone in order to take the copy of it. All of that, we would say, was tortious.
NETTLE J: You have damages for the conversion of the phone in manipulating it. You want not damages for that, but an injunction in effect deleting their copy of the information.
MR LLOYD: That is - - -
NETTLE J: It is not alleged to be confidential, and it does not sound as though it is to you. On what basis would there be an injunction mandatorily to compel them to delete it?
…
NETTLE J: What is the cause of action that underlies the injunction?
MR LLOYD: Damages is not an adequate remedy to us in the circumstances of this case. To undo the tort - destruction achieves the undoing of the tort.
EDELMAN J: You want to really say that the information is property that you want to treat in the same way as tangible property and it is property of your client.
MR LLOYD: Well, I do not think I have to go that far. It is sufficient that the [respondents] had put [themselves] into a position of having information which was in our possession only by reason of a series of torts in order to get that information. If we want relief in respect to undo that tort then, although damages can be a remedy, injunctions can also be a remedy to undo it and the damages does not provide us with useful or material relief in the circumstances of this case, unlike an injunction.
GORDON J: The difficulty about even assessing that contention is we do not know what this material is. It is not before the Court, so how does one make an assessment even at that level, assuming you are right in the way you have put your argument? You are asking for a mandatory injunction. One has to put into play a set of considerations and balances and work out where the balance lies, putting aside even the cause of action. You have two problems I think you need to address. One is Justice Nettle's question about the cause of action and the second is where is the balance? How do we assess the balance, absent fact? There is nothing in the special case directed at either of those issues.
MR LLOYD: I accept that, and I accept that the special case does not in terms say that there was a specific character of confidentiality to the material, but it is still material that can only be accessed by accessing the phones so it is, in that sense, confidential because it is not available to the world. It is not accessible to anyone. It requires the permission of the person who controls access to the phone.
EDELMAN J: You are really talking about tort of invasion of privacy then, are you not?
MR LLOYD: We are seeking relief to undo trespass to our property. Damages, in our case, is not an adequate remedy – damages is not an adequate remedy. Injunction is still available to provide a remedy for the tortious conduct.[7]

This exchange led to a fairly lengthy debate the following morning as to the court's power to grant an injunction requiring destruction of the copied data, including the following:

NETTLE J: … The difficulty here is, if I may say so with great respect, you have to identify a legal right or equitable right or statutory right in aid of which equity will grant relief in the auxiliary jurisdiction and thus far, as like yesterday, you have not done so.
MR LLOYD: Well, I suppose, your Honour, we would say that if that is true there then is a significant gap — and if I can explain that gap. We would say that if we get to the point where the court accepts that in advance of the tortious conduct it could provide relief, then it becomes a question of whether or not equity will provide no relief after the tortious conduct is done and in effect abandon the person who has suffered the tortious conduct which has ongoing consequences of tortious conduct.
KIEFEL CJ: Do you need to expand the notion of property then?
MR LLOYD: In my submission no, your Honour.
KIEFEL CJ: Because the difficulty is the information on the mobile phone has been taken and placed on property of the AFP and it seems to have lost its identity. In the olden days, back in the 1980s when search warrants were in vogue or became in vogue, we were only dealing with documents. It was easy to identify the property and it did not change in its nature. The difficulty is now technology and this has not really been addressed in the older search warrant cases because the question just did not arise.
MR LLOYD: I accept that that is so, but that is why we say that equity should be seen as able to give the relief we seek because otherwise you have a situation — one can posit a situation where there is a search warrant and the police take – half of the documents they take are originals and half the documents they do — they copy the documents.
Insofar as they take the originals there would be no doubt that there would be an ongoing property right to get those original documents back again. That is irrespective of confidentiality; just an ongoing right. But because in the second scenario the other half they have taken as copies, there is not a property right in the copies. We say in both cases equity can provide an injunctive relief to restore the person who has suffered the tort to the position they were in if damages is not an adequate remedy.
…
GORDON J: Can I just ask one question? There is an elephant in the room here. This gap that you identify is really you seeking to have us create a new rule, a new legal right. Is it any more than you seeking to have a new tort of privacy? I mean, in a sense you want *Lenah Meats* extended a bit, do you not?
EDELMAN J: Just to add to that, it seems to me that the work that is being done by the word "private" that you mentioned earlier is to exclude cases where the document contained, for example, information that was completely public so that I think you are trying to exclude the circumstance where that completely public information is copied and need not be returned.
MR LLOYD: Well, I am trying to say that, in the example I gave of the police taking half originals and half copies, we would say that equity should be able to and in fact can restore the person to the position they were in before the tort by returning both, whether or not there is property in the documents.

EDELMAN J: But I think Justice Gordon's question to you is that it is really the gap that you are talking about is really because the document contains private material, even if not confidential.
MR LLOYD: In the example I have just said it has nothing to do with whether those documents had private material. In both cases the documents are taken — tortiously taken — and that, we say, is enough. If we came to the Court prior to the tort, we would not say some of the documents are private and they should not be able to commit a tort because some documents are private. That would be irrelevant. The tort is the tort. We would get relief, irrespective of whether the documents were private or not.
EDELMAN J: So if the document were a newspaper you would say that the newspaper that was owned by the person whose house had been searched and was taken, there would be a right to get that back. But you would say that equity would also give a mandatory injunction to require copies that were taken of a public newspaper to be either destroyed or returned?
MR LLOYD: There may be strong discretionary reasons why you would not do it in that case, but we would say that equity could do it in a case where there were not discretionary reasons against it. The first point I have to get to is that equity at least has the ability to provide the relief. That is what I am trying to get to.
KIEFEL CJ: What is equity acting in aid of, though? On your scenario it is acting in aid of the law, is it not, rather than a private right — some more general notion of acting in aid of the law which - - -
MR LLOYD: To remedy the tortious conduct.[8]

The other basis on which the journalist argued that the court had power to grant an injunction requiring destruction of the copied data was based on public law decisions. In the *Johns v Australian Securities Commission*[9] (*Johns*) case, decided in 1993, the High Court held that where a statute confers an obligation on a person to produce documents or information to a public official for a purpose, there is an implied duty on the public official to only use the information provided under compulsion for the relevant purpose, or another purpose permitted by law, whether or not the information was confidential. That decision was not directly applicable to this case, because the *Johns* principle imposes limits on the right to use or disclose information that has lawfully come into the possession of a public official. Here, the journalist claimed that the copied data was obtained by an act of trespass. So the next steps in the journalist's argument were as follows:

- the allegedly unlawfully copied data should only be used and disclosed by police in the way permitted by the Crimes Act 1914 (Cth), especially the provisions relating to search warrants
- section 3ZQU of the Crimes Act sets out the permitted uses of information and things obtained under search warrants issued under the relevant part of the Crimes Act
- if the warrant in this case is invalid, in the eyes of the law it was not issued under the relevant part of the Crimes Act, therefore s 3ZQU does not permit any use of the allegedly unlawfully copied data, with the result that there are no permitted uses of the copied data
- as there are no permitted uses of the copied data, there is power to grant an injunction, subject to discretionary factors, to either prevent any use of the copied data by the police or to destroy the copied data

## The Attorney-General's response

In response to these arguments, the Attorney-General's position was that:

- in relation to the first proposed basis on which an injunction might be granted, an injunction should only be granted in to protect an established legal right, which did not exist in this instance
- the *Johns* argument did not assist the journalist because the police only propose to use the copied data for a purpose permitted by s 3ZQU, namely to investigate whether a serious crime has occurred

Further, even if the court had power to grant an injunction, the Attorney-General's argument was that, as a matter of discretion, no injunction ought to be granted because (1) there is a strong public interest in allowing an investigation into whether a serious crime has been committed to proceed, and (2) to require the police to cease that investigation would be inconsistent with the law of evidence that allows illegally obtained materials to be admitted into evidence in certain circumstances.

## Crystal ball gazing

Given the lack of evidence of the contents of the documents that were copied by the police, it seems unlikely that this case will be the one to decide whether Australian law recognises a tort of invasion of privacy. But there may be some non-binding commentary on the issue from the court.

In some ways, this case raises issues similar to the recent decision in the Paradise Papers case (*Glencore International AG v Cmr of Taxation*[10] (*Glencore*)), in which the High Court held that the Commissioner could use documents the subject of legal profession privilege, even though those documents had only come into the possession of the Commissioner after an unidentified hacker obtained unauthorised access to the IT system of the Bermudan law firm retained by Glencore, and published the documents on the internet.

In *Glencore*, the relief sought was an injunction to restrain use of the relevant documents and information

derived from them, coupled with an order for delivery up of copies of the documents held by the Commissioner. The court refused to grant an injunction, stating that Glencore's argument:

> ... rests upon an incorrect premise, namely that legal professional privilege is a legal right which is capable of being enforced, which is to say that it may found a cause of action.[11]

The fact pattern in *Glencore* is similar to that in *Lenah Game Meats*, in that the party against whom an injunction was sought had not been responsible for the trespass through which the information was obtained (that was the hacker in Glencore's case and the animal liberationist who installed a camera in the abattoir operated by Lenah Game Meats), whereas in this case the injunction is sought against the trespassers directly (the police).

In the absence of any evidence as to the contents of the documents that were copied, it is difficult to see the court granting an injunction requiring deletion of the copied documents simply because the copies were the fruit of an act of trespass. Had there been evidence that the copied files involved communications between the journalist and a confidential source obtained for the purpose of researching a potential newspaper article, there may have been a sound basis for arguing that the copying of such communications purportedly pursuant to an invalid search warrant would be an intrusion on the seclusion of the journalist's affairs that would be highly offensive to a reasonable person,[12] although it would have been strictly unnecessary to do so because the right to an injunction to protect confidential information is well established. Similarly, if there had been evidence that copyright in the copied documents had been owned by the journalist or her employer, there would have been a recognised cause of action to support the availability of an injunction, subject to discretionary considerations.[13] However, none of these arguments were possible because of the limited scope of the special case.

The argument based on *Johns* also has some parallels to the Paradise Papers case, although the documents had not been obtained by the Commissioner of Taxation pursuant to a statutory power. In that case, Keane J's interaction with Glencore's counsel drew out Glencore's position that the claim was to prevent any use by the Commissioner of the documents at all, "even if he uses them to get the right actual result".[14] Here, the journalist is asking the court to restrain the use of information for a purpose that would have been lawful, had the warrant been valid. For reasons of coherence in the law, it may be a step too far for the court to go this far, given that the law (both common law and statutory evidence law) recognises that illegally obtained documents may be admitted into evidence in appropriate cases.

***Patrick Gunning***
*Partner*
*King & Wood Mallesons*
*patrick.gunning@au.kwm.com*
*www.kwm.com*

## Footnotes

1. *Smethurst v Cmr of Police* [2019] HCATrans 216.
2. *Smethurst v Cmr of Police* [2019] HCATrans 223.
3. *Australian Broadcasting Corp v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199; 185 ALR 1; [2001] HCA 63; BC200107043.
4. A Smethurst "Annika Smethurst: AFP raid left my private world on display" *The Daily Telegraph* 9 June 2019 www.dailytelegraph.com.au/news/nsw/annika-smethurst-afp-raid-left-my-private-world-on-display/news-story/2bb4cefc340b848acf1d29ea69b87434.
5. High Court Rules 2004 (Cth), r 27.08.
6. *George v Rockett* (1990) 170 CLR 104; 93 ALR 483; BC9002921.
7. Above n 1.
8. Above n 2.
9. *Johns v Australian Securities Commission* (1993) 178 CLR 408; 31 ALD 417; BC9303583.
10. *Glencore International AG v Cmr of Taxation* (2019) 372 ALR 126; [2019] HCA 26; BC201907072.
11. Above n 8, at [12].
12. See above n 2, at [42] per Gleeson CJ and at [120] per Gummow and Hayne JJ.
13. Of course, if the journalist was in possession of a "leaked" document from the Commonwealth, copyright in that document would be owned by the Commonwealth and not by the journalist or her employer.
14. See *Glencore International AG v Cmr of Taxation of Commonwealth of Australia* [2019] HCATrans 82.

**For editorial enquiries and unsolicited article proposals please contact Genevieve Corish at genevieve.corish@lexisnexis.com.au or (02) 9422 2047**
**Cite this issue as (2019) 16(8) *PRIVLB***
**SUBSCRIPTION INCLUDES: 10 issues per volume plus binder www.lexisnexis.com.au**
**SYDNEY OFFICE: Locked Bag 2222, Chatswood Delivery Centre NSW 2067**
**CUSTOMER RELATIONS: 1800 772 772**
**GENERAL ENQUIRIES: (02) 9422 2222**
**ISSN 1449-8227 Print Post Approved PP 243459/00067** 