
# TOOLS OF THE TRADE - WHAT'S NEW IN THE TOOLBOX FOR AUSTRALIAN REGULATORS?

Companies and individuals are increasingly the target of regulatory investigations in Australia. Local regulators have long expressed frustration at the disparity between the options available to them when compared to their overseas counterparts. However, recent developments indicate a broadening of the suite of tools available to Australian regulators and the importance for companies to stay abreast of the changes.

**Key issues**

- Telephone intercepts have been used to convict three individuals of conspiracy to bribe a foreign public official
- It is now mandatory for telecommunication companies to keep metadata for two years – and regulators can access it without a warrant
- Reforms to Australia's whistleblower legislation seek to give more adequate protection in the private sector

## TELEPHONE INTERCEPTS

In September 2017, three individuals were convicted in Australia's first public sentence of conspiracy to bribe a foreign public official following a guilty plea shortly before trial. The defendants were not the original targets of the investigation; investigators were looking into their business associate when they happened upon intercepted telephone conversations involving the planned bribing of Iraqi officials. These intercepts provided much of the evidence gathered by prosecutors.

The initial basis for the intercepts was not entirely clear as the *Telecommunications (Interception and Access) Act 1979* (Cth) requires a "serious offence" for an intercept warrant. Once calls are lawfully intercepted, however, they are generally admissible in other proceedings. The individuals involved were sentenced to imprisonment of up to four years and two were fined.

This decision is a timely reminder of the permissible use of telephone intercepts and other telecommunications data in identifying criminal activity.

## DATA ACCESS

In Australia, regulators are able to access certain customer information required to be kept by telecommunication companies for a period of two years. Recent legislative amendments mandate the dataset that must be stored. Regulators are able to access this information through a variety of methods to assist in investigations including stored communications warrants, which can provide access to the content of emails and SMS messages. Regulators can also use telecommunications data authorisations, for access to metadata.

Metadata access is available to enforcements agencies if it is "reasonably necessary" and authorised, without even requiring a warrant. Whilst metadata won't give away the content of conversations, it does indicate individual phone numbers of the parties to the conversation, the timing, and the length. Call

logs will also disclose the frequency of contact. This information can be particularly important to investigators as a fundamental building block of their case.

## WILL IT SOON BE SAFER TO BLOW THE WHISTLE?

Regulators are assisted by whistleblowers, particularly in situations where detection of wrongdoing is notoriously difficult. Australian lawmakers have long been criticised for the lack of protection in place for private sector whistleblowers, which creates a culture of silence (see our previous publication: https://www.cliffordchance.com/briefings/2016/09/culture_of_silencedoesaustralia.html).

In October 2017, draft legislation was released which aims to address the current inadequacies together with a public consultation (https://consult.treasury.gov.au/market-and-competition-policy-division/whistleblowers-bill-2017/). The proposed legislation creates a defined "whistleblower regulated entity", expands on the class of persons covered (to include family members) and the types of disclosures that can be made. Confidentiality protections are also expanded with greater financial sanctions. The proposed legislation does not yet include US style rewards for whistleblowers whose information yields results for regulators.

## PREPARATION AND TRAINING

Up-to-date staff training is essential to ensure compliance with the changing landscape. If your company has operations outside Australia, common role-playing scenarios should involve money laundering or bribery to help employees appreciate the real risks involved.

Staff should understand that phone calls, texts, and emails create a permanent record. Staff may not realise that their personal activity on company email may be subjected to production to a regulator if it falls within the terms of a search warrant or production notice. An email to a friend about a development at work, something the individual never intended to amount to tipping off, may lead to an investigation of insider trading.

Often front-of-house staff are not trained in how to react when a regulator comes knocking. Consider training for all front-of-house staff as to what to look out for, who to call, and what to do if a warrant is served. Consideration should be given to protect legal professional privilege, and material not within the scope of the warrant. Records should be kept of everything removed from the office.

Increasingly, companies need to separate the legal representation of the company from that of key individuals. Companies often have a law firm or panel of firms available to them if a crisis occurs but neglect to have a plan for their staff. Consider preparing a list of preferred law firms that senior members of staff can access if independent legal representation is required when they are approached by a regulator. While these law firms do not owe any obligation to the company, competent and adequate employee representation protects not only their rights but may also prevent inadvertent and unnecessary disclosures against the company's interests.

CLIFFORD CHANCE

## CONCLUSION

In an increasingly regulated world, corporate bodies must ensure compliance practices are up-to-date and relevant. With regulators showcasing their new and expanded investigative tools, companies must ensure that a culture of compliance is established and emphasised throughout the company.

# CONTACTS

**Jenni Hill**
Partner

**T** +61 8 9262 5582
**E** jenni.hill@cliffordchance.com

**Wendy Wysong**
Partner

**T** +852 2826 3460
**E** wendy.wysong@cliffordchance.com

**Diana Chang**
Partner

**T** +61 2 8922 8003
**E** diana.chang@cliffordchance.com

**Kirsten Scott**
Counsel

**T** +61 8 9262 5517
**E** kirsten.scott@cliffordchance.com

**Kate Godhard**
Counsel

**T** +61 2 8922 8021
**E** kate.godhard@cliffordchance.com

**Lara Gotti**
Associate

**T** +61 8 9262 5518
**E** lara.gotti@cliffordchance.com