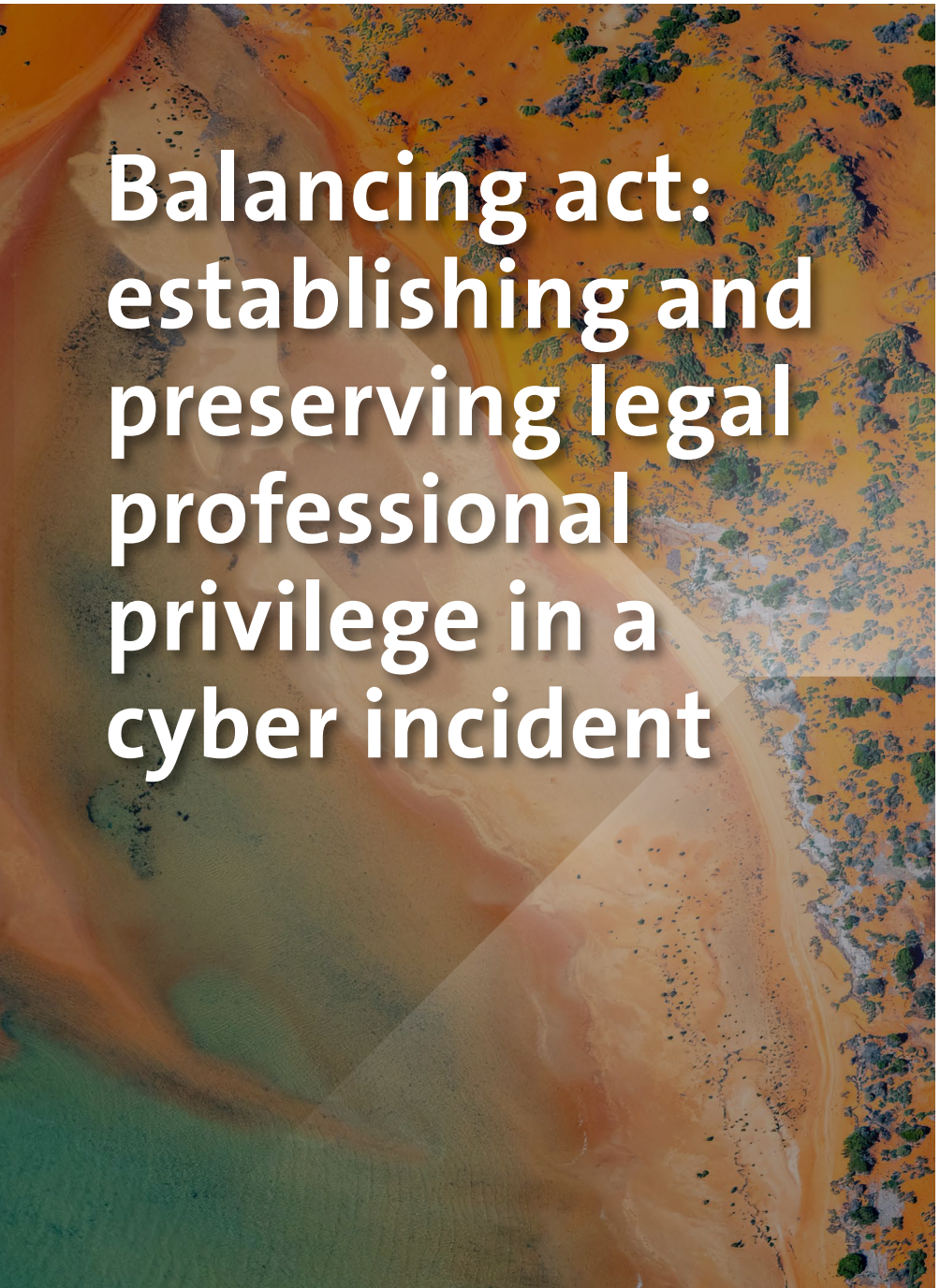
Allens

In alliance with Linklaters



Balancing act: establishing and preserving legal professional privilege in a cyber incident

Taking steps to maintain legal professional privilege in a cyber incident is an important risk management measure

As part of its investigation into a major cyber incident it suffered late last year, Optus procured a report from Deloitte that investigated the cause of the incident and related matters. In class action proceedings against Optus, the group members sought access to that report. Optus refused to produce the report on the basis that it was subject to legal professional privilege (***LPP***). On 10 November 2023, the Federal Court handed down its decision on this issue, finding that the report was not subject to LPP.

This is the first time a claim for LPP in relation to an investigation report into a cyber incident has been tested in court in Australia, but it likely won't be the last.

Cyber incidents have unique characteristics that can make it especially difficult to claim or preserve LPP over documents generated in response, particularly forensic investigation reports. But given cyber incidents are increasingly exposing organisations to expensive litigation and regulatory enforcement action, *taking steps before and during an incident to maximise the prospect of LPP attaching to communications—both by increasing the body of evidence to support any claim and by reducing the risk of inadvertent waiver of LPP—is itself an important risk management measure*.

Of course, attempts to claim or preserve privilege shouldn't get in the way of the security of an organisation. However, it is possible to significantly reduce the friction that might otherwise be introduced by incorporating privilege preservation measures into your cyber *readiness* activities.

In this guide we explain:

- **the importance of LPP in the context of escalating litigation and regulatory enforcement action**
- **the challenges of claiming it in the cyber-incident context**
- **key actions to take, elements to consider and questions to ask.**

For a more detailed analysis of the Optus decision, see our Insight:
Optus decision highlights challenges for privilege claims over investigation reports.

Managing privilege: key actions to take

1 Develop a cyber incident privilege policy

that:

- outlines the practical steps your organisation should take in relation to specified activities and documents, to maximise the prospect of claiming LPP, reduce the risk of inadvertent waiver and reduce the friction that may be introduced to preserve LPP (where it exists) in the wake of a cyber incident
- includes template artefacts (eg privilege protocols for the cyber incident response team and external cyber experts) that can be easily circulated in an incident.

2 Update your cyber incident response plans

to embed privilege considerations and include trigger events for contacting legal in respect of an incident.

3 Brief your cyber incident response team

on the importance of maintaining LPP, ways to reduce the risk of waiver and the operation of your organisation's privilege policy.

4 Get legal involved early on in an incident

and be clear about the advice required and the internal and external inputs required to inform that advice or assist with anticipated litigations.

5 Take care when relying on documents created by inhouse counsel

Reports and documents prepared by inhouse counsel are more likely to be found to lack the 'dominant' purpose of legal advice and instead have a range of purposes, especially when they are acting in a capacity other than as legal counsel (which is common in inhouse roles).

6 Be prepared to point to evidence

Clear, focussed, specific and compelling evidence from key decision-makers (which may include the general counsel, CEO, board members etc) about their understanding and intentions will be critical to the court's decision on whether a privilege claim can be sustained.

> *'It is not sufficient to show a substantial purpose or that the privileged purpose is only one of two or more purposes of equal weighting...It must be the paramount or most influential purpose. One practical test is to ask whether the communication would have been made (whether the document would have been brought into existence) irrespective of the obtaining of legal advice'.*[1]

Note: Taking these actions will not guarantee your organisation's ability to claim that relevant communications are privileged or that LPP has not been waived. These issues will always be determined on a case-base-case basis having regard to the dominant purpose test, the circumstances in which a communication or document was created, and whether confidentiality has been preserved.

1 *Robertson v Singtel Optus Pty Ltd* [2023] FCA 1392 [88] quoting *Asahi Holdings (Australia) Pty Ltd v Pacific Equity Partners Pty Ltd (No 4)* [2014] FCA 796 at [28] to [44].

Legal professional privilege

What is legal professional privilege?

Legal professional privilege protects from disclosure (such as to a regulator or other party in litigation) confidential communications or documents made for the dominant purpose of:

- ***advice privilege*** – seeking or giving legal advice; or
- ***litigation privilege*** – obtaining advice in relation to, or the preparation of evidence or documents for use in existing or anticipated litigation.

This is the ***dominant purpose test***.

Why does LPP matter?

Cyber incidents – which often shine a light on deficient cybersecurity and data-handling practices – are increasingly exposing organisations to litigation and regulatory enforcement action.

For example, in 2022-2023:

- *penalties* for serious or repeated interferences with privacy have increased to the greater of $50 million, three times the value of the benefit obtained attributable to the breach or, if the court cannot determine the value of the benefit, 30% of the adjusted turnover of the body corporate during the turnover period for the contravention.
- *five data breach class actions* were commenced against Optus and Medibank (although these have now been consolidated into three class actions that remain on foot). We anticipate that the likely introduction of a direct right of action for breaches of the Privacy Act as part of upcoming privacy reforms will significantly increase data breach class action activity in Australia.
- APRA imposed additional capital requirements of $250 million on Medibank, reflecting weaknesses identified in Medibank's information security environment following the cyber incident it experienced in late 2023. APRA also recently announced it will take strong action to enforce compliance with CPS234.
- *ASIC* successfully brought proceedings against RI Advice for its failure to manage cybersecurity risks and cyber resilience.
- *cyber insurers* have recently broadened key exclusions in cyber insurance policies.

What is the challenge?

Cyber incidents have unique characteristics that can make it especially difficult to claim LPP and, where it does exist, easy to inadvertently waive in the heat of a crisis:

- **time pressure** – cyber incidents generally require that organisations act quickly to contain the incident and mitigate the potential impacts. Rapid containment of, and recovery from, the incident is typically a priority, and creating significant delays by introducing undue friction can exacerbate the impact.
- **ease of disclosure** – cyber incidents often involve a large number of people within the business and a range of external experts—all of whom require varying levels of information. This can make it hard to keep privileged information confidential.
- **prescriptive regulation** – regulation and guidance on how organisations respond to cyber incidents is becoming increasingly prescriptive, making it hard to delineate between communications or documents created for the dominant purpose of legal advice or anticipated proceedings, and those created for the dominant purpose of managing the incident (including to comply with regulatory requirements or risk management points).
- **relevance of cyber forensics to broader response** – cyber forensic analysis, including root-cause investigation, is often required to inform the business' broader response to the incident (including remediation and preventative measures), as well as to inform legal advice. It will be important to consider whether one, broad-based investigation is appropriate, or whether two reports should be procured that delineate between the aspects of the investigation that are more clearly for the dominant purpose of legal advice and those falling within the scope of the privileged investigation.

Questions and considerations

Types of legal advice that may be required

Understanding the areas of legal advice that may be required in connection with a cyber incident can help identify which documents typically need to be created for the purpose of that legal advice or anticipated litigation.

This can include:

- **stakeholder engagement** – advice on whether (and how) to notify and engage with regulators, government agencies, members, contractual counterparties, insurers / brokers and other stakeholders (including the contents of such notifications and what other information and documents should / shouldn't be disclosed to them).
- **legality** – advice on whether the actions taken in response to the cyber incident are permitted by law (eg paying a ransom, certain investigative activities, purchase of data posted on the dark web etc).
- **assessments** – advice on how to undertake personal information and sensitivity assessments in order to discharge regulatory and contractual obligations such as regulatory and contractual notification requirements.
- **exposure and liability** – advice on legal exposure in connection with the incident (eg past compliance with the law, potential liability to third parties, potential liability of third parties, obligations to remediate, and obligations to change systems and processes).
- **insurance** – advice on coverage available under cyber insurance policies, including potentially in relation to payment of a ransom (if applicable).
- **directors' duties** – advice on board compliance with directors' duties.
- **litigation and regulatory action** – advice on potential or actual litigation (eg shareholder / member class actions) and regulatory action (eg from the OAIC, ASIC, APRA etc).
- **remediation** – advice on recommended uplifts to enable compliance and reduce legal risk.

Key documents for consideration include:

- cyber incident response team agendas and minutes
- board papers and updates to the board
- cyber response team communications channel
- forensic expert reports and status updates
- threat intelligence
- internal and external communications
- correspondence with your cyber insurer/broker
- ransom negotiation transcripts
- compromised data assessment methodology and decision logs
- post-incident review reports
- ad hoc legal advice

Ask...

- **Is the communication confidential?**
- **Was litigation reasonably contemplated at the time the communication or document was created?**
- **Was the document created to give or obtain legal advice?**
- **Was the communication created for the *dominant purpose* of either the litigation or giving or obtaining legal advice?**

Key contacts

Valeska Bloch
Partner, Head of Cyber
T +61 2 9230 4030
Valeska.Bloch@allens.com.au

Gavin Smith
Partner, Co-head of Corporate, Head of Technology, Media and Telecommunications
T +61 2 9230 4891
Gavin.Smith@allens.com.au

David Rountree
Partner
T +61 7 3334 3368
David.Rountree@allens.com.au

Jonathan Light
Partner
T +61 2 9230 4423
Jonathan.Light@allens.com.au

Chris Kerrigan
Partner
T +61 2 9230 4208
Christopher.Kerrigan@allens.com.au

Isabelle Guyot
Managing Associate
T +61 2 9230 4752
Isabelle.Guyot@allens.com.au

Lauren Holz
Senior Associate
T +61 2 9230 4283
Lauren.Holz@allens.com.au

Andrew Burns
Senior Associate
T +61 3 9613 8118
Andrew.Burns@allens.com.au