QUAY INSIGHTS

April 2025

Don't waive goodbye to privilege: How to maintain legal professional privilege in the context of a data breach

Organisations focus on detection, containment, investigation and notification obligations in the context of data breaches. In the midst of taking those steps, including dealing with a threat actor, recovering personal information and other data, as well as complying with different legal obligations, entities may lose sight of the need to protect legal professional privilege in the documents that are created. This article unpacks the Federal Court's decision in *McClure v Medibank Private Limited* [2025] FCA 167, which provides useful guidance for how to preserve privilege over reports that are prepared in the context of data breach responses.

McClure v Medibank Private Limited [2025] FCA 167

1. Medibank engaged both lawyers and cybersecurity advisory firms to assist with its response to a major cybersecurity incident that affected 9.7 million customers and former customers in the later part of 2022. Deloitte was appointed to conduct a review of the data breach, including to undertake a post-incident review, assess the root causes of the data breach and, finally, consider Medibank's compliance with the Australian Prudential Regulation Authority's (**APRA**) Prudential Standard CPS 234. Ultimately, Deloitte produced three reports (**Deloitte Reports**).

2. The applicants in a class action against Medibank sought production of certain reports and communications related to the data breach, including the Deloitte Reports. Medibank objected to production of many of those reports and communications, including the Deloitte Reports, on the basis of a claim of legal professional privilege (**LPP**). While the judgment considered whether the other reports and communications were subject to LPP, it is the comments of Rofe J in relation to the Deloitte Reports that are of most interest.

3. A party to legal proceedings asserting a claim of LPP bears the onus of establishing that LPP applies. As Rofe J pointed out in his decision (at [176]) for LPP to be successfully claimed in respect of any communication, that communication must be confidential and *made for the dominant purpose of giving or obtaining (including preparing for obtaining) legal advice or legal services, including obtaining legal representation in proceedings.* His Honour (at [178]) referred to three key principles, as set out in Singtel Optus Pty Ltd v Robertson [2024] FCAFC 58, which were of critical importance in this case:

(a) the purpose for which a document is created is to be determined objectively on the basis of available facts, including a consideration of the nature of the document and submissions made by the parties;

(b) the intent of the person creating the document is not determinative; and

(c) that obtaining legal advice or assistance is a *substantial* purpose is not sufficient – that purpose must be the predominant or paramount purpose.

4. While Medibank argued that the Deloitte Reports were produced for the primary purpose of allowing Medibank's lawyers to provide legal advice to assist in responding to potential litigation regarding the data breach and ultimately to act for Medibank in that litigation, if it eventuated, the Federal Court found that – having regard to the totality of the information available – the Deloitte Reports were in fact produced for a number of "equally dominant" purposes, not limited to obtaining legal advice and assistance, but also including at least:

(a) ASX/PR purposes, that is, to satisfy the ASX and investors that it was addressing the breach and also to satisfy other stakeholders that Medibank was seeking to protect the personal information of its customers; and

(b) APRA purposes, primarily to ensure that APRA would not undertake its own independent investigation by ensuring that the Deloitte investigations satisfied the information needs of APRA.

5. As Rofe J pointed out, Medibank had the onus of establishing the basis of the LPP claim, which onus was not discharged and, accordingly, the LPP claim failed.

6. The key facts that the Federal Court took into account in making this decision were (noting Rofe J determined, at paragraph [191], that the time for ascertaining purpose was when the report was commissioned, though it was also possible to look at subsequent events):

(a) that Medibank for a period from approximately the point Deloitte was first engaged referred to the Deloitte work in its ASX announcements and other public communications, including by stating that Deloitte had been appointed by Medibank, not its lawyers, that the work was being done to protect customers and to learn from the incident and committing to share the results of the review. In fact, the Deloitte Reports were the only external reviews that Medibank publicly referred to;

(b) that Medibank sought APRA's approval to Deloitte's appointment and the terms of Deloitte's review, in an effort to seek to ensure that APRA's information requirements were met, in other words, Medibank sought to ensure that APRA would not undertake its own review. The correspondence between Medibank and APRA as to the scope of the review indicated only a very minor role was played by Medibank's lawyers in settling the terms of the review. In addition, APRA was involved in meetings with Deloitte and was provided with a copy of all of the Deloitte Reports;

(c) the board of directors directly commissioned the Deloitte Reports and both board members and other non-legal staff were very involved in the progress of the Deloitte Reports. Rofe J concluded that the board wanted to understand in an "unvarnished" sense what occurred, wanted direct reporting from Deloitte, not Medibank's lawyers, and wanted to be seen by stakeholders as treating the data breach very seriously;

(d) Medibank's lawyers did have access to the Deloitte Reports, to understand the nature of the breach in non-technical terms, to understand what information had been taken, to also understand the steps that were being taken to mitigate the risks that a similar breach might occur in the future and, finally, to consider the question of compliance with CPS 234. However, particularly in light of the fact that those lawyers had access to reports prepared by other experts, this was a significant but not the dominant purpose of obtaining the Deloitte Reports; and

(e) the CEO of Medibank notified the ASX that it had been provided with Deloitte's findings from its post incident report and would be implementing Deloitte's recommendations that had not yet been implemented. Further, all three Deloitte Reports were discussed at board meetings at which not only board members but a range of senior Medibank executives who were not lawyers were present.

7. For completeness, the Federal Court found that Medibank would, in any event, have waived privilege in part of the first of the Deloitte Reports. In short, the test for waiver of LPP (which, again, is a factual test, having regard to all of the circumstances) is whether a party has acted in a manner that is inconsistent with a claim of privilege. Rofe J found that, through its public statements regarding the conclusions of the first of the Deloitte Reports, that Deloitte had made recommendations to enhance Medibank's IT processes and systems, Medibank had waived privilege in that report. As stated by Rofe J at paragraph [445]:

> *Medibank was seeking to take advantage of its implementation of the recommendations resulting from the external incident review conducted by Deloitte to deflect criticism and enhance or maintain its good standing in the eyes of its shareholders and customers and its share price. It cannot at the same time maintain privilege in that part of the report setting out the recommendations to enhance Medibank's IT processes and systems. I consider that by making the statements in the 28 April 2023 ASX Announcement, Medibank has waived privilege in that part of the PIR Report relating to the recommendations to enhance Medibank's IT processes and systems.*

8. Waiver was also supported by the significant involvement that APRA had with both shaping the instructions to Deloitte, the development of the Deloitte Reports and the fact that those reports were provided to APRA, which APRA was free to use for the purposes of any regulatory action it chose to take.

Key Takeaways

9. The Federal Court's findings in relation to the Deloitte Reports provide useful guidance as to what steps should be taken if LPP is to be maintained in a report commissioned in the wake of a data breach:

(a) Ensure that the lawyers appointed to assist with the data breach are the ones that actually commission the report and provide instructions to the consultant preparing the report.

(b) Do not make public statements that directly refer to either the fact that the specific report has been commissioned or the consultant that has been appointed and, to avoid waiver of LPP, do not directly reference the findings of the report.

(c) Ensure the report is provided to the lawyers appointed to assist and not directly to the board or senior management.

10. Of course, if it is the case that a report is commissioned for purposes other than legal advice or assistance, ensure that the instructions provided to the relevant consultant are appropriately limited to cover only what is required for those other purposes.

Contacts

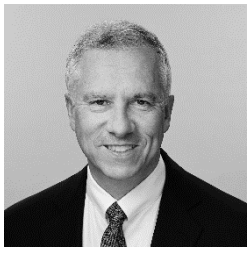
Angela Flannery
Partner

Quay Law Partners
Level 32, 180 George Street,
Sydney NSW 2000

T +61 419 489 093
E angela@quaylaw.com
www.quaylaw.com

Cate Cloudsdale
Counsel

Quay Law Partners
Level 32, 180 George Street,
Sydney NSW 2000
T +61 461 477 550
E cate@quaylaw.com
www.quaylaw.com



Dave Poddar
Partner

Quay Law Partners
Level 32, 180 George Street,
Sydney NSW 2000
T +61 422 800 415
E dave@quaylaw.com
www.quaylaw.com