PUBLICATION

Privilege Under Fire: Protecting Forensic Reports in the Wake of a Data Breach

Authors: Matthew George White, Alexander Frank Koskey, III, Madison J. McMahan
May 19, 2025

In the chaos following a cyberattack, forensic reports are often pulled together under intense pressure and can assist companies in responding to and remediating the incident. However, if you're not careful, these reports might do more damage in the courtroom than the threat actor did to your network. What many organizations don't realize – until litigation begins – is that these reports can quickly become prime targets for discovery. Without careful planning to ensure forensic engagements and resulting reports are properly structured and shielded under the attorney-client privilege and/or work product doctrines, they may end up in the hands of opposing counsel in data breach litigation.

A recent decision from the Federal Court of Australia in *McClure v. Medibank Private Limited* [2025] FCA 167 underscores just how easily privilege can be lost. While McClure was decided under Australian law, the court's reasoning closely aligns with a series of U.S. cases that have steadily narrowed protections for forensic reports in recent years. The key takeaway from these decisions is clear: privilege doesn't only depend on who commissioned the report – it hinges on why it was created, how it was used, and who saw it.

Forensic reports often reveal detailed technical findings and expose security vulnerabilities that could significantly influence the outcome of litigation. Protecting these reports under the attorney-client privilege or the work product doctrine isn't just a best practice – it's a critical step in managing legal risk after a breach. Left unprotected, a forensic report can serve as a roadmap for plaintiffs, outlining the very vulnerabilities and response gaps they'll use to build their claims.

McClure v. Medibank

The case stems from a 2022 data breach that impacted millions of Medibank customers and prompted a class action lawsuit alleging failures in cybersecurity safeguards. As part of discovery, plaintiffs sought a range of materials prepared in response to the breach, including forensic reports from Deloitte and other third-party vendors. Medibank resisted production, claiming that the reports were protected by privilege because they were created to support litigation strategy and enable legal advice.

The court agreed in part, upholding privilege over reports commissioned by counsel for threat actor negotiations and legal strategy. However, it ordered the production of three Deloitte reports, finding that they were created for multiple purposes and that obtaining legal advice was not the dominant one.

The court's analysis focused on several critical facts:

- **Public positioning**: In press releases and ASX announcements, Medibank described Deloitte's role as being related to customer protection, governance, and transparency – not legal advice.
- **Regulatory messaging**: Medibank told regulators that Deloitte was engaged to avoid a separate investigation by the Australian Prudential Regulation Authority (APRA), further supporting a nonlegal purpose.

- **Board reporting**: Deloitte reported directly to Medibank's board and executive team, not to external counsel, which suggested the work was for operational oversight rather than legal strategy.

- **Public Statements:** Medibank publicly referenced and implemented Deloitte's recommendations, which the court said undercut any claim of confidentiality and waived privilege.

Ultimately, the court concluded that while legal advice was *a* purpose of the reports, it was not *the* dominant one required to sustain privilege. An appeal of this decision is likely.

A Broader Legal Trend

The *McClure* decision echoes a growing trend in U.S. courts: forensic reports are losing privilege protection when their primary legal purpose isn't clearly established and thoroughly documented.

In the U.S., courts have taken similar approaches in high-profile breach litigation:

- In *Guo Wengui v. Clark Hill, PLC* (D.D.C. 2021), the court held a law firm's forensic report was discoverable despite being routed through outside counsel, because the investigation was ultimately deemed business continuity work and not legal preparation. The report had been widely shared and used operationally.

- Likewise, in *In re Capital One Consumer Data Sec. Breach Litig.* (E.D. Va. 2020), the court rejected privilege claims over a forensic report prepared by Capital One's on-retainer cybersecurity vendor, even though it had been commissioned by counsel. The scope of work had remained unchanged from preexisting business arrangements, and the court noted that the report was paid for by the IT department and shared extensively internally and with regulators.

These cases all highlight the same cautionary tale: when forensic reports serve dual purposes – or appear primarily intended to support business operations rather than legal strategy – claims of privilege stand on shaky ground. Courts are increasingly scrutinizing the true purpose of these reports, and superficial involvement of legal counsel is often insufficient. Experienced data breach counsel can play a critical role in structuring the investigation from the outset to preserve privilege, including by directing the engagement of forensic experts, clearly documenting the legal purpose of the work, and limiting the distribution of the report to those who need them for legal decision-making. These steps, among others, can mean the difference between a report that supports your defense and one that becomes the plaintiff's roadmap.

Practical Tips: Protecting Privilege in Cyber Investigations

Based on the decisions in *McClure*, *Clark Hill*, *Capital One*, and others, here are steps companies can take to better protect forensic reports:

1. **Engage vendors through counsel**. Outside legal counsel should retain and direct forensic vendors. Engagement letters should clearly state that the purpose is to obtain legal advice and prepare for potential litigation.

2. **Separate legal and operational workstreams**. Consider using different vendors (or teams) for business continuity and legal defense. If using one vendor, structure distinct scopes of work, teams, and reports for legal and non-legal purposes.

3. **Avoid dual messaging**. Be careful with public statements, board updates, or regulator communications. Suggesting that a report serves governance or PR functions may undermine

privilege claims.

4. **Restrict report access**. Limit distribution of legal reports to individuals directly supporting counsel and only on a "need to know" basis. If broader distribution is needed, consider preparing a separate, non-privileged version.

5. **Avoid putting analysis into the mitigation report**. When preparing the non-privileged investigation report for purposes of mitigation, attorneys and companies should ensure that no analysis or interpretation is included in the report. Discussion of next steps, effects of the breach, and characterizations of the attack that may occur in the mitigation investigation should remain in oral format until findings are solidified. Once finalized, such findings should be presented either in the legal investigation report or in a privileged attorney letter.

6. **Follow the money trail**. Courts examine who pays for the work. Legal reports should be billed to and paid by legal departments, not IT or operations.

7. **Plan for privilege from day one**. Privilege can't be retroactively applied. Bring in experienced data breach counsel at the start of any investigation and set up processes to maintain clear legal oversight.

The *McClure* decision is the latest reminder that form alone does not preserve privilege – courts are looking for substance. Even reports routed through legal channels may have to be produced if they are ultimately used for business, governance, or regulatory purposes. Organizations that fail to distinguish between legal and operational workstreams risk having their most sensitive investigative materials used against them in court.

In today's high-stakes and rapidly evolving litigation landscape, early and strategic planning isn't optional – it's essential. Engaging experienced outside counsel from the outset can make all the difference in structuring your incident response and vendor relationships to preserve privilege and minimize litigation risk. Baker Donelson's Cybersecurity Incident Response Team has guided clients through some of the most complex data breach responses across all industries. Let us help you put the right legal protections in place – before the subpoenas start flying.

If you need guidance on establishing procedures to protect privilege, responding to a cybersecurity incident, or defending against data breach litigation, don't hesitate to contact the authors, Matt White, Alex Koskey, or MJ McMahan, or any other member of Baker Donelson's Incident Response Team. We regularly assist clients in navigating these high-risk moments with clarity, efficiency, and strategic focus. Our team also advises on a broad range of cybersecurity, data privacy, and technology matters – whether proactive or reactive. We're here to help.