Dispute Resolution and Knowledge Management

21 April 2025

South Africa

Chatting away your protection – Are you waiving legal privilege when you use AI?

For more insight into our expertise and services

Chatting away your protection – Are you waiving legal privilege when you use AI?

Generative artificial intelligence tools such as ChatGPT, Claude and Copilot, to name a few, have become a routine feature of modern business operations. Today's executives and employees increasingly use these tools to summarise documents, brainstorm strategies, draft correspondence, analyse risks and mitigate exposure. Yet the rapid adoption of artificial intelligence (AI) raises an urgent and largely unresolved question for South African clients: can the use of AI tools compromise the legal privilege that protects confidential communications with lawyers?

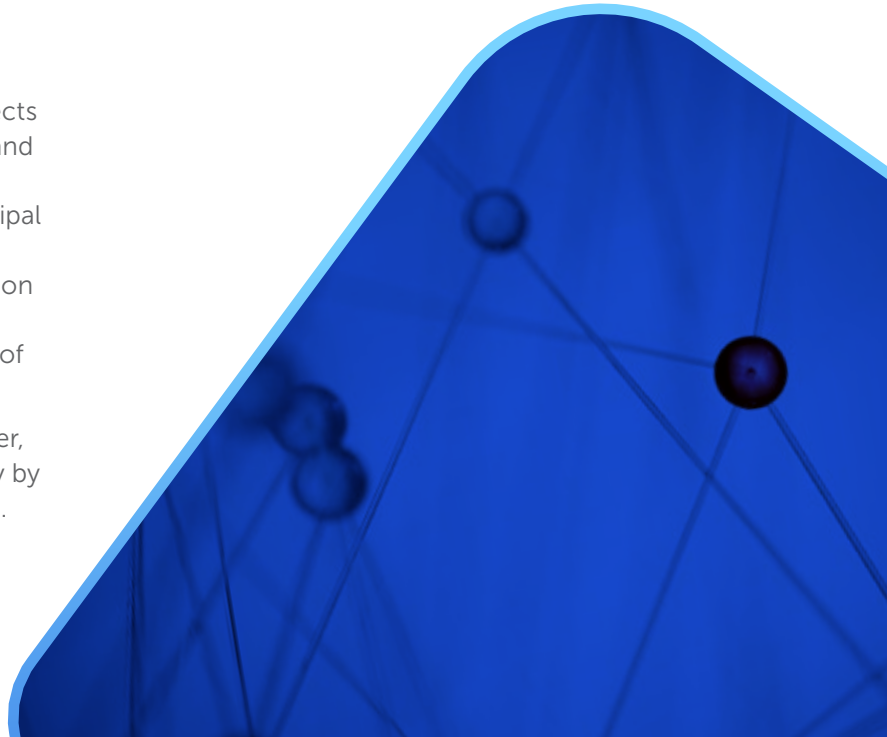
South African law does not yet have a definitive judicial pronouncement on this issue. However, the foundational principles of legal professional privilege in South Africa, which are rooted in the common law and closely aligned with English legal tradition, provide a clear framework for analysing these risks. Recent developments abroad, most notably the landmark ruling by Judge Rakoff of the United States District Court for the Southern District of New York in *United States v Heppner*, as well as cautionary remarks from the United Kingdom's Upper Tribunal of the Immigration and Asylum Chamber (Tribunal), offer powerful illustrations of how these risks can materialise in practice.

This article examines the intersection of generative AI usage and legal privilege through a South African lens, drawing on comparative jurisprudence to highlight the practical steps clients should take to protect their privileged communications.

The foundations of legal privilege in South Africa

Legal professional privilege in South Africa protects confidential communications between a client and their lawyer made for the purpose of seeking or giving legal advice. This encompasses two principal branches: legal advice privilege, which applies whether or not litigation is underway, and litigation privilege, which protects communications and documents prepared for the dominant purpose of pending or contemplated litigation.

The privilege belongs to the client, not the lawyer, and can (with limited exceptions) be waived only by the client's conduct, whether express or implied. Critically, waivers occur when the substance of privileged material is disclosed to a third party outside the privileged relationship. It is not strictly necessary for the client to make the disclosure to the third party. In certain circumstances, the lawyer's conduct may also amount to a waiver of the client's privilege. Once confidentiality is lost, for instance, if privileged information enters the public domain, the privilege falls away and cannot be reasserted.



The court in *The South African Airways SOC v BDFM Publishers (Pty) Ltd and Others* (2015/33205) [2015] ZAGPJHC 293 underscored this point: once a legally privileged in-house legal memorandum had been released into the public domain, whether such release was authorised or not, its privileged nature cannot be relied upon to prevent its publication by media houses, because privilege is a right to refuse disclosure in legal proceedings, not a positive right to protect or preserve the information from dissemination.

These principles, while well established, take on new significance in the context of AI. The central question is whether inputting legally privileged information into a generative AI platform constitutes a disclosure to a third party and, if so, whether that disclosure destroys the legal privilege attached thereto.

***United States v Heppner*: A cautionary tale**

The most instructive authority to date is the February 2026 ruling in *United States v Heppner*, which Judge Rakoff described as addressing *"a question of first impression nationwide"*. The case arose in the context of a criminal prosecution for securities and wire fraud. Bradley Heppner, following his receipt of a grand jury subpoena and while clearly the target of a federal investigation, independently used Anthropic's consumer AI chatbot, Claude, to generate over 30 documents that outlined defence strategy and potential legal arguments. *Heppner* subsequently shared these documents with his lawyers and asserted that they were protected by attorney-client privilege and the work product doctrine, which protects trial preparation materials for or by a litigant in the United States.

Judge Rakoff rejected both claims. On the question of privilege, the court identified three independent grounds for its ruling. First, the communications were not between Heppner and his attorney, given that Claude is not a lawyer and no attorney-client relationship existed. The court emphasised that all recognised privileges require *"a trusting human relationship"* with *"a licensed professional who owes fiduciary duties and is subject to discipline"*, and no such relationship could exist between a user and an AI platform.

Second, the communications were not confidential. Anthropic's privacy policy, to which all Claude users consent, provides that Anthropic collects data on both user inputs and AI outputs, may use such data for model training, and reserves the right to disclose information to third parties, including governmental regulatory authorities. In the court's view, submitting information under these terms was fundamentally inconsistent with maintaining a reasonable expectation of confidentiality.

Third, Heppner did not communicate with Claude for the purpose of obtaining legal advice. Although his counsel asserted that Heppner used Claude for the *"express purpose of talking to counsel"*, Heppner had not done so at counsel's direction. The court held that the relevant question was whether Heppner intended to obtain legal advice from Claude, however, Anthropic's privacy policy itself disclaimed any ability to provide such advice.

On the work product doctrine, the court similarly found no protection. Heppner had acted on his own volition, not at the behest of his counsel, and the documents did not reflect his counsel's strategy at the time of their creation. The court concluded that non-privileged documents cannot be *"alchemically changed into privileged ones upon being shared with counsel"* after the fact.

It bears emphasis that *Heppner* does not stand for the proposition that AI use can never be privileged. As McDermott Will & Schulte LLP noted in a recent article published in *Lexology*, the ruling is "*best understood as a technology-neutral decision applying longstanding privilege principles to a new context*". If the attorney had directed the client to use an enterprise AI tool behind the legal adviser's firewall, with appropriate confidentiality protections and training disabled, the analysis might well have been different. The *Harvard Law Review*, in a detailed critique of the judgment, argued that Judge Rakoff's reasoning "*veers toward categorically excluding a client's use of generative AI from attorney-client privilege*" and that a more fact-dependent approach would be preferable. The critique draws attention to the manner in which clients routinely use third-party platforms such as Gmail, Google Docs, and iCloud to communicate with lawyers without courts questioning whether those tools defeat privilege.

Implications under south African Law

Although *Heppner* is a United States decision and not binding in South Africa, its reasoning closely mirrors the doctrinal pillars that underpin South African legal professional privilege. The parallels are significant.

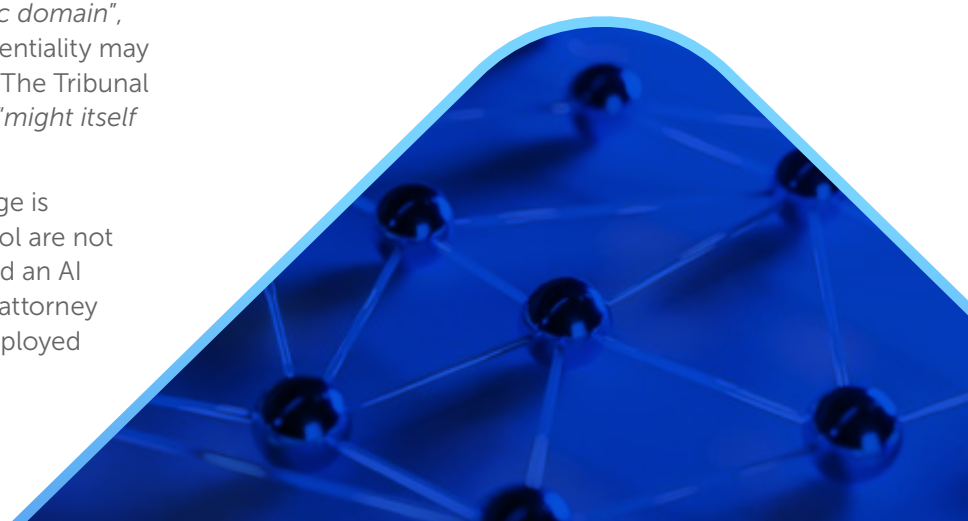
Under South African law, privilege requires that a communication be made on a confidential basis, with a lawyer (i.e. an advocate, attorney or qualified in-house legal adviser acting in a professional capacity), for the purpose of seeking or obtaining legal advice. When a client or their lawyer enters information into a public AI chatbot, each of these elements is placed at risk.

The confidentiality requirement is the most immediately vulnerable. South African privilege law is clear that voluntary disclosure to a third party outside the privileged relationship generally constitutes a waiver. A consumer AI platform whose terms of service permit data retention, model training and disclosure to regulators is, in functional terms, a third party, and any information entered or uploaded by a client, would be considered to be a voluntarily disclosure to a third party. Heppner's reasoning on this point – that the platform's own privacy policy defeated any reasonable expectation of confidentiality – would translate directly into the South African analysis.

The Tribunal recently reinforced this concern, stating that uploading confidential documents into an open-source AI tool such as ChatGPT or Claude places the information "*on the internet in the public domain*", with the consequence that client confidentiality may be breached and legal privilege waived. The Tribunal added that uploading such information "*might itself warrant referral to the regulatory body*".

Similarly, the purpose element of privilege is affected. Communications with an AI tool are not communications with a legal adviser, and an AI platform cannot be characterised as an attorney or an agent of an attorney unless it is deployed under a lawyer's supervision and within a controlled workflow. The fact that a client subsequently shares AI-generated outputs with a legal adviser does not retroactively clothe those materials with privilege.

In the context of litigation privilege, similar risks arise. South African litigation privilege covers communications and documents prepared for the dominant purpose of anticipated litigation, but the materials must be prepared by or at the direction of a legal adviser, or at least within the framework of the attorney-client relationship. Materials independently generated by a client using a public AI tool, without a legal adviser's involvement, are unlikely to satisfy this requirement as was demonstrated in the *Heppner* judgment.



Practical guidance for clients

The convergence of these principles yields several important practical recommendations for South African businesses and individuals who use or intend to use AI tools in connection with legal matters:

Distinguish between public and enterprise AI tools

Enterprise AI platforms deployed behind a firm's firewall, with contractual protections against data retention and training, present a lower risk. Where a legal adviser supervises such use, privilege arguments are stronger. Key factors include whether the platform guarantees confidentiality, whether training is disabled and whether a legal adviser directs the workflow.

Do not upload privileged or confidential information into public AI tools

Free-to-use platforms typically retain user data, use it for model training or share it with third parties, either of which may waive privilege. Singapore's Guide for Using Generative AI in the Legal Sector recommends avoiding confidential information in such tools altogether, alternatively anonymising data where use is unavoidable.

Ensure lawyer involvement from the outset

One of the decisive factors in *Heppner* was that Heppner used Claude of his own volition, without direction from a lawyer. If AI tools are to be used in connection with any contemplated or pending litigation, investigations and reports for purposes of obtaining advice on pending or contemplated litigation, or for seeking legal advice, that use should be initiated and supervised by a lawyer. As the McDermott commentary observed, documenting that AI use is at the direction of a lawyer and within a controlled workflow may be critical to preserving both privilege and work product protection.

Engage legal advisers on their use of AI

Clients should engage their lawyers on whether AI tools are being used, which tools are used and the safeguards around that use (including data retention, training, access controls and human review). This is both a risk-management and privilege-preservation step. It helps ensure that any AI-assisted work is carried out within a controlled workflow, aligned to confidentiality obligations and consistent with the client's expectations and internal policies.

Review and update internal AI policies

Organisations should ensure that their AI use policies expressly prohibit the sharing of confidential and privileged information with public AI models. Employee training should emphasise that communicating with an AI chatbot is not equivalent to speaking with a legal adviser, and that doing so may irrevocably compromise privilege.

Read the terms of service

Before using any AI platform for matters touching on legal advice or strategy, users should review the provider's data handling, retention, and disclosure policies. The presence or absence of confidentiality protections in those terms would determine whether legal privilege is maintained. Users should also consider whether the terms of service can be changed without notice to them, as this may also affect the protection provided for legally privilege information.

Conclusion

The use of generative AI in business is here to stay, and its capacity to enhance productivity and decision-making is undeniable. However, as the *Heppner* judgment and the Tribunal's remarks clearly illustrate, the traditional principles governing legal privilege apply with full force to AI interactions. South African legal professional privilege rests on the same foundational requirements of confidentiality, a qualifying legal relationship and a legal advice purpose: each of these can be undermined by the incautious use of AI tools.

While the technology may be new, the principles governing privilege are not. Preserving privilege in the age of AI requires the same discipline that has always been required when engaging third parties: purpose, legal professional involvement and an unwavering commitment to confidentiality. Clients who adopt these practices, and embed them in organisational policy and training, will be well positioned to harness the benefits of AI without forfeiting the legal protections on which effective legal representation depends.

Anja Hofmeyr, Calinka Murray and Safee-Naaz Siddiqi

OUR TEAM

For more information about our Dispute Resolution practice and services in South Africa, Kenya and Namibia, please contact:

Rishaban Moodley
Practice Head & Director:
Dispute Resolution
Sector Head:
Gambling & Regulatory Compliance
T +27 (0)11 562 1666
E rishaban.moodley@cdhlegal.com

Tim Fletcher
Chairperson
Chief Risk Officer
Director: Dispute Resolution
T +27 (0)11 562 1061
E tim.fletcher@cdhlegal.com

Patrick Kauta
Managing Partner | Namibia
T +264 833 730 100
M +264 811 447 777
E patrick.kauta@cdhlegal.com

Imraan Abdullah
Director:
Dispute Resolution
T +27 (0)11 562 1177
E imraan.abdullah@cdhlegal.com

Timothy Baker
Director:
Dispute Resolution
T +27 (0)21 481 6308
E timothy.baker@cdhlegal.com

Eugene Bester
Director:
Dispute Resolution
T +27 (0)11 562 1173
E eugene.bester@cdhlegal.com

Neha Dhana
Director:
Dispute Resolution
T +27 (0)11 562 1267
E neha.dhana@cdhlegal.com

Denise Durand
Director:
Dispute Resolution
T +27 (0)11 562 1835
E denise.durand@cdhlegal.com

Claudette Dutilleux
Director:
Dispute Resolution
T +27 (0)11 562 1073
E claudette.dutilleux@cdhlegal.com

Jackwell Feris
Sector Head:
Industrials, Manufacturing & Trade
Director: Dispute Resolution
T +27 (0)11 562 1825
E jackwell.feris@cdhlegal.com

Nastascha Harduth
Sector Head: Corporate Debt,
Turnaround & Restructuring
Director: Dispute Resolution
T +27 (0)11 562 1453
E n.harduth@cdhlegal.com

Anja Hofmeyr
Director:
Dispute Resolution
T +27 (0)11 562 1129
E anja.hofmeyr@cdhlegal.com

Annemari Krugel
Director:
Dispute Resolution
T +27 (0)11 562 1709
E annemari.krugel@cdhlegal.com

Mercy Kuzeeko
Director:
Dispute Resolution
T +26 (4)83 373 0100
E mercy.kuzeeko@cdhlegal.com

Corné Lewis
Director:
Dispute Resolution
T +27 (0)11 562 1042
E corne.lewis@cdhlegal.com

Nomlayo Mabhena-Mlilo
Director:
Dispute Resolution
T +27 (0)11 562 1743
E nomlayo.mabhena@cdhlegal.com

Sentebale Makara
Director:
Dispute Resolution
T +27 (0)11 562 1181
E sentebale.makara@cdhlegal.com

Vincent Manko
Director:
Dispute Resolution
T +27 (0)11 562 1660
E vincent.manko@cdhlegal.com

Khaya Mantengu
Director:
Dispute Resolution
T +27 (0)11 562 1312
E khaya.mantengu@cdhlegal.com

Richard Marcus
Director:
Dispute Resolution
T +27 (0)21 481 6396
E richard.marcus@cdhlegal.com

Lebogang Makwela
Director:
Dispute Resolution
T +27 (0)11 562 1057
E lebogang.makwela@cdhlegal.com

Burton Meyer
Director:
Dispute Resolution
T +27 (0)11 562 1056
E burton.meyer@cdhlegal.com

Desmond Odhiambo
Partner | Kenya
T +254 731 086 649
+254 204 409 918
+254 710 560 114
E desmond.odhiambo@cdhlegal.com

Lucinde Rhoodie
Director:
Dispute Resolution
T +27 (0)21 405 6080
E lucinde.rhoodie@cdhlegal.com

Clive Rumsey
Sector Head: Construction & Engineering
Director: Dispute Resolution
T +27 (0)11 562 1924
E clive.rumsey@cdhlegal.com

Belinda Scriba
Director:
Dispute Resolution
T +27 (0)21 405 6139
E belinda.scriba@cdhlegal.com

Tim Smit
Sector Head:
Consumer Goods, Services & Retail
Director: Dispute Resolution
T +27 (0)11 562 1085
E tim.smit@cdhlegal.com

Joe Whittle
Director:
Dispute Resolution
T +27 (0)11 562 1138
E joe.whittle@cdhlegal.com

Roy Barendse
Executive Consultant:
Dispute Resolution
T +27 (0)21 405 6177
E roy.barendse@cdhlegal.com

Rimo Benjamin
Counsel:
Dispute Resolution
T +27 (0)11 562 1716
E rimo.benjamin@cdhlegal.com

Randhir Singh
Counsel:
Dispute Resolution
T +27 (0)11 562 1704
E randhir.singh@cdhlegal.com

BBBEE STATUS: LEVEL ONE CONTRIBUTOR
Our BBBEE verification is one of several components of our transformation strategy and we continue to seek ways of improving it in a meaningful manner.

PLEASE NOTE
This information is published for general information purposes and is not intended to constitute legal advice. Specialist legal advice should always be sought in relation to any particular situation. Cliffe Dekker Hofmeyr will accept no responsibility for any actions taken or not taken on the basis of this publication.

JOHANNESBURG
1 Protea Place, Sandton, Johannesburg, 2196. Private Bag X40, Benmore, 2010, South Africa.
Dx 154 Randburg and Dx 42 Johannesburg.
T +27 (0)11 562 1000 F +27 (0)11 562 1111 E jhb@cdhlegal.com

CAPE TOWN
11 Buitengracht Street, Cape Town, 8001. PO Box 695, Cape Town, 8000, South Africa. Dx 5 Cape Town.
T +27 (0)21 481 6300 F +27 (0)21 481 6388 E ctn@cdhlegal.com

NAIROBI
Merchant Square, 3rd floor, Block D, Riverside Drive, Nairobi, Kenya. P.O. Box 22602-00505, Nairobi, Kenya.
T +254 731 086 649 | +254 204 409 918 | +254 710 560 114
E cdhkenya@cdhlegal.com

ONGWEDIVA
Shop No A7, Oshana Regional Mall, Ongwediva, Namibia.
T +264 (0) 81 287 8330 E cdhnamibia@cdhlegal.com

STELLENBOSCH
14 Louw Street, Stellenbosch Central, Stellenbosch, 7600.
T +27 (0)21 481 6400 E cdhstellenbosch@cdhlegal.com

WINDHOEK
2nd Floor, 4@Steps - East Tower, Hilltop Estate, Kleine Kuppe, Windhoek.
PO Box 97115, Maerua Mall, Windhoek, Namibia, 10020
T +264 833 730 100 E cdhnamibia@cdhlegal.com

CLIFFE DEKKER HOFMEYR | cliffedekkerhofmeyr.com