

Pause Before You Prompt: NY Court Finds AI-Generated Content Is Not Privileged

March 4, 2026

Authors

[Ilya Smith](#), [Myriah V. Jaworski](#), [Chirag H. Patel](#)

In what appears to be a first of its kind [ruling](#), a federal district judge (Hon. Jed S. Rakoff, Southern District of New York) on February 17, 2026 held that AI-generated information, that relied on privileged inputs, is not protected by attorney-client or work product privilege.

Among other factors, the Court considered the AI tools' privacy policy which allowed disclosure of user inputs and outputs to "government regulatory authorities" and to other "third parties" in certain situations. Interestingly, these terms may exist even in enterprise versions of AI tools.

While the ruling relates to highly nuanced facts and should be read narrowly, it highlights risks that should be considered by organizations wishing to protect confidential information while increasingly relying on AI to work smarter.

Facts

The defendant, the founder and former CEO of a financial services startup, is [charged](#) with securities fraud and other related crimes alleged to have resulted in his obtaining \$150 million through fraud. Purportedly after an investigation had begun but before being indicted, the defendant "conversed" with an Anthropic Claude AI tool^[1] sharing "inputs" which the AI tool used to generate 31 documents, the "outputs." The Government discovered these AI generated outputs while executing a search warrant at the defendant's home.

The defendant asserted that these AI generated outputs were protected by attorney-client and work product privilege because: (a) the inputs included information the defendant had learned from his

attorneys, and (b) that the defendant used the AI solution to prepare reports on strategies for his potential defense in the course of working with his attorneys.

The Government moved the Court for a finding that the AI generated outputs were not entitled to attorney-client or work product protection.

Attorney-Client Privilege and Work Product

Attorney-Client Privilege. The Attorney-Client Privilege (ACP) protects communications that are –

- (1) between a client and his or her attorney;
- (2) that are intended to be, and in fact were, kept confidential; and
- (3) for the purpose of obtaining or providing legal advice[2].

The defendant's primary argument was that the AI generated outputs were created for the purpose of obtaining legal advice from his attorney.

The Government attacked the first and second prongs of ACP by arguing that the AI generated outputs were not created by an attorney and were not intended to be confidential. The Government relied heavily on the AI solution's [privacy policy](#), which stated that the AI tool was allowed to disclose the defendant's personal data (including as appearing in inputs and outputs) to "government regulatory authorities" and to other "third parties."

The Court agreed with Government and emphasized in its [bench ruling](#) that the AI tool "expressly provided that users have no expectation of privacy in their inputs." The Court acknowledged that defendant's inputs to the AI tool may have been privileged. However, the Court focused its inquiry on defendant's use of the AI tool, and construed that use as a communication with a third-party (not with an attorney).

Work Product Doctrine. The facts of the case worked against a finding that the Work Product Doctrine protected the 31 AI documents. The Work Product protections did not attach, the Court ruled, because the defendant created the AI documents on his own initiative and not at the direction of his attorneys and the documents did not reflect the attorneys' legal strategy at the time that they were created thereby undercutting the policy reasons for Work Product protections.

Takeaways

1. A client is at risk of waiving Attorney-Client Privilege when it shares privileged information with an AI tool independent of their attorney's direction.

In the bench hearing, the Court observed that an AI solution is a third party between a client and their attorney. Additionally, privilege only attaches if communications are for the purpose of

obtaining or providing legal advice. Organizations should remember that disclosures to a third party or to individuals within an organization that do not have a “need to know” may sever legitimate privilege protections.

- **DO** understand that clients cannot make AI-generated material privileged by simply forwarding it to counsel.
- **DO NOT** use AI tools without your attorney’s direction to record information, perform legal analysis, or produce records that contain confidential information.
- **DO** keep tight control of the internal individuals and third-parties who may receive Attorney-Client Privileged communications or Work Product.
- **DO** put protocols in place to guard against unintentionally waiving privilege by disclosing attorney communications.
- **DO NOT** assume that just because an in-house or external attorney is present at a meeting recorded or processed by an AI tool, the content of the AI-generated recording or document will be privileged.
- **DO NOT** record or use AI tools to process attorney’s legal advice.

2. Know your commercial privacy rights but assume no privacy/confidentiality in inputs or outputs.

The Court’s reliance on the government disclosure exception in a privacy policy to find waiver raises an interesting question as such language exists in the privacy policy of many AI tools and other software (including enterprise versions). However, it is important to remember unique facts of this case – a client inputting privileged information into a public tool in which the AI tool also expressly disclaimed confidentiality.

Nonetheless, this case provides an important reminder to carefully evaluate the privacy policies and terms of use in an enterprise setting. AI solution terms of service may provide you with property interests in the inputs and outputs and the privacy policy may provide for only limited disclosures to third parties and significant privacy rights as between a user or organization and the AI company. Exercising such privacy rights (e.g. right of deletion) may help a corporation reduce the risk of later discovery or disclosure.

- **DO** understand how your information will be used or when it may be disclosed by an AI tool by reading the Privacy Policy and Terms of Service.
- **DO** carefully review and negotiate confidentiality and disclosure provisions in enterprise tools. Perform privacy and security due diligence before authorizing use of an AI solution. Just like all AI technologies are not created equal, each may differ in terms, privacy policies and security controls.
- **DO NOT** permit confidential corporate information or personal information to be shared with an AI Tool as an input.

- **DO** think again about using AI tools to record confidential communications (i.e. AI notetakers in meetings).
- **DO** understand that even if not disclosed intentionally, the AI solution may fall victim to a cyber breach and there are no security guarantees that the information will remain protected.
- **DO** create and enforce an AI policy allowing your personnel, agents, and service providers to use only approved AI solutions for approved uses.

Organizations should consult their legal counsel before utilizing AI tools across their company, particularly in connection with legal strategy and sensitive communications, and implement clear guardrails moving forward. If you have any questions on the content of this alert or the use of AI-generated content, contact a member of the Clark Hill [Artificial Intelligence & Emerging Technologies](#) team.

This publication is intended for general informational purposes only and does not constitute legal advice or a solicitation to provide legal services. The information in this publication is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this information without seeking professional legal counsel. The views and opinions expressed herein represent those of the individual authors only and are not necessarily the views of Clark Hill PLC. Although we attempt to ensure that postings on our website are complete, accurate, and up to date, we assume no responsibility for their completeness, accuracy, or timeliness.

[1] It is not clear from the record which Claude AI solution the defendant used but the Government references the Privacy Policy applicable to the solution made available through the Claude.ai website as opposed to the various Claude enterprise AI products, each of which presumably have their own privacy and terms of service.

[2] US v Mejia 655 F3d 126, 132 (2d Cir. 2011)



Related Industries

Artificial Intelligence & Emerging Technologies

Related Practice Areas

Data Privacy, Protection & Cybersecurity

Related

Legal Updates

February 2026 Global Immigration Recap | APAC

Clark Hill's Global Immigration team provides an overview of the major updates from February 2026 in the Asia-Pacific region.

Legal Updates

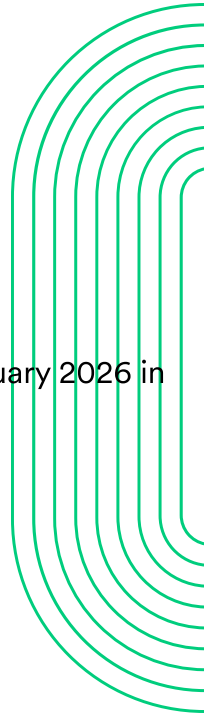
February 2026 Global Immigration Recap | EMEA

Clark Hill's Global Immigration team provides an overview of the major updates from February 2026 in the Europe, Middle East, Africa region.

Legal Updates

February 2026 Global Immigration Recap | Americas

Clark Hill's Global Immigration team provides an overview of the major updates from February 2026 in the Americas region.



Also of Interest:

[Empower Your Professional Success](#)

[We Practice The Law As It Should Be: Simply Smarter.](#)

[Other Services](#)



The Clark Hill approach is equally pragmatic and growth-minded, which is why we understand our clients' toughest business challenges. Our multidisciplinary, global team of advisors focuses on smart legal solutions, delivered simply.

[Contact Us](#)



[Policies & Disclaimers](#)



[Client Log-in](#)



[Payments](#)

© 2026 Clark Hill PLC.