The Ethics and Security Risks of AI Note-Takers in the Workplace

Jacob McCarthy, Skyler Sax, Justice Ishio, Justin Gonzalez and Shreyas Kumar
Texas A&M, College Station, USA

jmccar18@tamu.edu
sax@tamu.edu
jmgonzalez@tamu.edu
justiceishio@tamu.edu
shreyas.kumar@tamu.edu

Abstract: The rapid adoption of Generative Artificial Intelligence (AI) has led to its deep integration into daily work environments, with AI note-takers emerging as a popular tool for transcribing and summarizing meetings using advanced Natural Language Processing (NLP). While these systems enhance workplace efficiency by providing real-time transcripts and concise summaries, they also introduce significant cybersecurity and ethical risks. Chief among these are questions of data ownership, third-party data sharing, and compliance with consent laws. In jurisdictions with two-party or all-party consent requirements, the deployment of AI note-takers raises legal challenges when participants are not fully informed or have not consented to being recorded. Moreover, consent mechanisms across AI platforms are inconsistent and often buried in complex disclosures, leading to uninformed use and potential violations of privacy. These risks are compounded by the opaque data practices of many AI companies, which may retain or monetize recorded conversations. This paper conducts a comprehensive analysis of privacy policies from leading AI note-taker providers, legislative frameworks across U.S. states, academic literature, and recent investigative reports. We identify key policy gaps and technical oversights that could compromise user trust, organizational data security, and regulatory compliance. Case studies are presented to illustrate both the productivity gains and the harms—such as unauthorized data exposure—that result from AI note-taker misuse. We conclude by offering targeted recommendations for policymakers, developers, and organizational decision-makers to mitigate ethical and security risks. These include harmonizing consent practices, enhancing user transparency, and enforcing stricter data governance standards. Our findings aim to promote responsible innovation and ensure that the deployment of AI note-takers is aligned with ethical principles and privacy rights in modern workplaces.

Keywords: Note-Takers, End user license agreement, Artificial intelligence (AI), Cybersecurity, Security risks

1. Paper Overview

1.1 Conceptual Framework

This paper takes the view that artificial intelligence (AI) is both a powerful tool for maximizing productivity and a potential risk to user privacy, especially when used in AI-powered notetaking tools. The focus is on the specific risks these tools introduce during virtual meetings, where sensitive conversations are often recorded and stored automatically.

A study by Majeed and Hwang (2023) helps frame this concern. They explain how synthetic data, which is information generated by AI to mimic real data, can act as adversarial background knowledge. Even though this synthetic data is not directly taken from users, it can be similar enough to real data that attackers might detect patterns, rebuild anonymized datasets, or even identify individuals. This creates serious privacy risks when proper protections are not in place.

We apply that same idea to AI note-taking tools used in video-calling platforms such as Zoom or Microsoft Teams. These tools often record and transcribe meetings without people fully realizing what is being stored or how it might be used later. That lack of clarity raises concerns about consent, data ownership, and how long this information is kept. Because of this, our paper also considers important ethical ideas such as informed consent, transparency, and privacy by design when evaluating how these tools are used.

1.2 Novelty and Innovation

This paper explores a part of AI privacy that has not received much attention. It focuses on the cybersecurity and ethical risks of AI-powered note-taking tools. While there has been an increase in research about AI and the ethics that surround it, very few studies directly examine the risks of data breaches or the ethics of storing personal data through transcription systems. Most existing research discusses areas such as surveillance and anonymization, but it rarely looks at the unique risks of utilizing AI note-taking tools. These tools record conversations passively, process them in real time, and store them long term. This project is one of the first to study this specific use of AI.

This work is different because it connects technical analysis with real-world insights, including Gartner's 2025 forecast, which predicts that 40 percent of AI-related data breaches by 2027 will come from the misuse of generative AI. This highlights how urgent and critical these concerns are becoming. The paper also uses the findings of Majeed and Hwang, who describe how synthetic data can be used in ways that threaten privacy. In addition, it includes an ethical analysis that focuses on informed consent, transparency, and accountability.

The purpose of this paper is to help users, developers, and organizations understand the hidden risks that come with using AI tools in everyday work settings. By addressing technical problems and ethical challenges, this paper encourages the development of safer AI systems and legal regulations that protect user privacy.

2. Problem Background

2.1 Review of Prior Events

According to ChatGPT in early June of 2025, the five top AI note-takers are Notion AI, Otter.ai, Fireflies.ai, Granola, and Google's NotebookLM. In late June of 2025, the Notetaking AIs mentioned by ChatGPT have changed to Otter.ai, Fireflies.ai, Fathom, Sembly AI, and Supernormal reflecting the constant shifting landscape of the AI market. Highlighting how fast the Generative AI landscape is developing and thereby compounding the larger issue of governmental legal systems' inability to advance at the same pace in order to maintain regulations.

On June 11th 2025, Disney and Universal filed a lawsuit against the AI firm Midjourney over the use of their copyrighted characters for training Midjourney's AI intelligence. Claiming that Midjourney is plagiarising their work through its online AI service, with a key point of Disney's argument being Midjourney has received financial gain from creating images of Disney and Universal's copyrighted works. In contrast, Midjourney is citing that their AI is simply a tool and how users utilize the system is up to them citing the United States' fair use policy as their defense. The outcome of this litigation could reshape how Image Generative AI is used throughout the United States as issues over AI plagiarism of artwork have been around since the inception of Image Generative AI. This litigation comes figuratively late in the game, as Midjourney's Image Generative AI program has celebrated its three year anniversary on July 12, 2025. OpenAI's DALL-E Image Generative AI program is even older, having been released back in 2021 to much fanfare.

Court cases regarding whether or not AI Generated work can be copyrighted first began appearing in August of 2023, two years after AI Image Generators first hit the open market. In Thaler vs Perlmutter, the court determined that "only human beings qualify as authors under U.S. copyright law, meaning that an AI-generated work like the one submitted by Thaler is not eligible for copyright protection." (*Thaler v. Perlmutter*, 2023). The gap between the rise of Image Generating AI and when legal cases started to appear highlights the slowness of the legal system in catching up to ethical issues related to AI. At the moment, there are no standard practices for the operation of such AI note-taking systems, and in certain cases such as in legal or medical settings, issues may arise regarding patients and attorney-client privilege and the Protected Health Information (PHI) of patients respectively. In a legal setting, it can also become difficult to conclude who has data ownership over the audio recordings once the meeting has come to an end.

2.2 Limitations in Existing Approaches

The previous litigation surrounding Generative AI can be used as a case study for AI Notetaking software, especially with the recent acquisition of Scale AI by Meta. However, we will first start with tech company privacy policies as it is no secret that various companies such as Google, Microsoft, and Facebook, now Meta, track user activities and sell that data to third party companies for targeted advertising. A particular climax of this issue came in 2018 with Mark Zuckerberg's senate hearing. This hearing took place after the Cambridge Analytica data breach where Cambridge Analytica harvested the data of millions of facebook user profiles to then build a software program to influence and predict decisions at the ballot box. Questions were raised regarding how much data Meta captures from their users, what that data is used for, and how transparent the whole process is to users. The end result of the hearing led to no major legislation or regulation changes outside of increased federal scrutiny of tech companies and Facebook having to pay 5 billion dollars in fines for misleading users about just how much (or how little) privacy they have over their data. Especially considering the AI note-taking companies utilize the same type of privacy policies as other tech companies.

Upon review of the privacy policies of the first set of AI Note-takers, many of the issues that led to the aforementioned 2018 hearing still persist. For example, the AI note-taking company Fireflies.ai collects device and usage data alongside any information provided over the use of their tools. They are then free "to provide you with further information and offers from us or third parties that we believe you may find useful or interesting, such as newsletters, marketing or promotional materials.” (Fireflies.ai, 2025) This allows Fireflies to sell user data to advertisers similar to what social media platforms such as Facebook and Instagram do. Otter.ai has a similar privacy policy where they provide their advertising partners with your data for targeted ads and analytics providers storing the personal data as long as necessary to fulfill the purposes of their privacy policy.

NotebookLM, a creation of Google, follows Google's privacy policy which allows for the collection of “the content you create, upload, or receive from others when using our services. This includes things like email you write and receive, photos and videos you save, docs and spreadsheets you create, and comments you make on YouTube videos.” (Google, 2025) Providing that data to Google’s affiliates and personalizing ads to a user. Meeting summaries and notes collected by NotebookLM would fall under this category. All of these privacy policies run into the questionable ethics of collecting so much information on the users of one’s system and the cybersecurity risks of utilizing AI note-takers. What happens when an adversary taps into the AI note-taker company’s cloud and makes off with last week's meeting notes? Or the information is improperly handled as in the case of Cambridge Analytica? Under current rules and regulations, these companies are only required to alert users of data breaches but housing all that user information does result in a large amount of cybersecurity risk on the part of the user. This issue has been thrust into the limelight recently with the class action lawsuit filed against Otter.ai on August 15th of 2025. The plaintiff, Justin Brewer, alleges the note-taker “deceptively and surreptitiously” recorded private conversations to train the tech company’s transcription service. Furthermore, there have been complaints by users that the AI joins meetings automatically when the service is linked to workplace calendars. Immediately recording those meetings without user consent which is a clear privacy and compliance violation. Clearly showing that ethics are not properly being taken into account by AI note-taking companies.

Ethical issues and legal grey areas arise as AI note-takers become more mainstream as well. Some states have all-party or two-party consent states, which require the consent of each individual before it can be recorded. As shown in the recently filed Otter.ai legal case. With the standard practice of notifying users that an AI note-taker is being utilized in a meeting and not being universal to alert, there may be issues that increase if there are disputes across state lines or even internationally. Employees, partners, and clients may be unaware they are being recorded by AI tools, eroding trust if disclosed after the fact. With an already rocky territory, things can get even trickier when taking into account the user information associated with AI note-taking users and the direct correlation to what adversaries would target and seek.

3. System Design / Theoretical Framework

3.1 Architecture / Model Description

In our theoretical model of properly implemented AI note-taker ethics practices, the AI note-taker acquires conceptual space alongside existing virtual-meeting software, tuning in to the live audio stream. Feeding it into a generative AI summarization and transcription process. The system would insert a standardized "AI present" message into the meeting UI before any words are recorded or processed—similar to how mute/unmute icons are inserted—so all attendees clearly know that an automated listener has joined. After recognizing the alert, the sound passes through a black-box model (like a cloud-based Transformer) that converts speech to text, condensed into action-item summaries. Most importantly, we layer on top a consent-gating module: unless all participants explicitly give their consent via an in-UI prompt, their microphone is effectively muted to the AI pipeline. Conceptually, consent records and transcript snippets would be authored to an encrypted audit log, keeping a permanent chain of who agreed and when, independent of any tangible backend yet.

3.2 Key Design Decisions

Since this is a proposal for proper AI note-taker ethics rather than a deployed system, our design choices favor clarity and ethical "bake-in" over engineering detail. We've chosen an in-UI banner and modal dialog style of consent rather than email or post-meeting checkbox, to offer real-time awareness. We put the "AI present" notification at the top of the participant list, making it as noticeable as any human participant, and tie the microphone unmuting to consent acceptance—so you can't speak until you've acknowledged the AI. In doing so as a black box treatment of the generative engine, we circumvent model-specific implementation and focus instead on data flows and user interactions. Finally, our audit-log concept logs timestamped consent events and every summary generation call so that any retrospective audit can trace back exactly who gave consent to be recorded and what sections of conversation the AI processed.

3.3 Proposed Tools, Techniques, and Data

In place of code writing or system building, our methodology relies on:

- (1) Review of literature and policy—examining API documentation, privacy notices, and consent-law laws
- (2) UX/flow prototyping—authoring screen mockups to demonstrate how consent dialogs and notifications would appear
- (3) Scenario modeling—creating prototype meeting transcripts (single-language and multilingual) to experiment with how and when consent gates and notifications would trigger
- (4) Expert consultation—gathering feedback from privacy officers and meeting-platform engineers on feasibility and user experience.

3.4 Experimental or Analytical Approach

To validate the suggested framework, we perform comparative policy analysis, comparing existing AI-note policies with our consent-gated design and identifying where there are deficiencies. We also perform scenario walkthroughs, simulating mock meetings in which consent is withheld, given partially, or withdrawn afterward to analyze how the system would behave. Utilizing first NotebookLM then Fathom.ai, we tested these capabilities during our team tag up meetings to see how the AI system complied with US consent laws and determine what level of cybersecurity risk the note-taker represented if misused. Together, these analyses will indicate both the practical virtues of our proposal as well as the tension underlying seamless user experience versus demanding ethical compliance.

4. Results and Analysis

4.1 Evaluation Criteria

The evaluation of AI note-taking tools was based on privacy impact assessment principles and focused on three main areas. These include the risk of unauthorized data access or sharing, the extent to which users were properly informed and gave consent, and how the system would respond if an attacker tried to exploit it using AI-generated synthetic data as background knowledge.

While we assess the cybersecurity, ethical, and legal risks and issues that surround AI notetaking, we must consider the following to accurately decipher this largely uncertain topic area:

First, the harmonization and standardization of consent practices and user information policies is a key part to ensure informed consent from users regarding the handling of their sensitive information. It should also be reviewed if a state is a two-party or all-party consent state, and if so, how that would impact privacy policies moving forward.

Second, enhancing user transparency, and enforcing stricter data governance standards is another component that drives many of the ethical issues we found. For someone to use a software that inherently has many cybersecurity risks that may impact users directly, it is important that they know what they are putting themselves at risk for. In this we must also consider one's vulnerabilities to adversarial attacks.

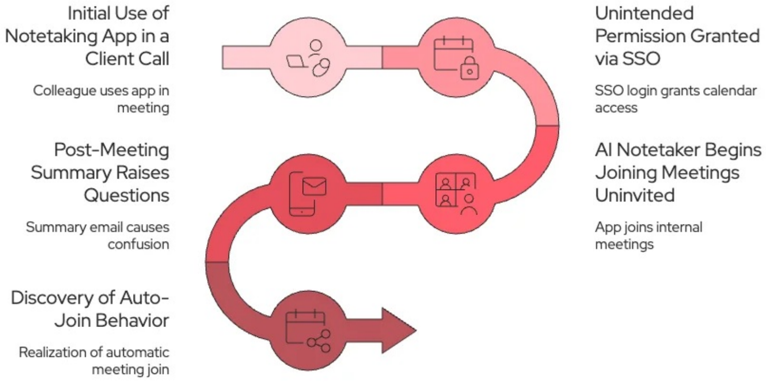
4.2 Observations and Outcomes

Recent studies have shown that AI Note-taking tools are vulnerable to attacks where adversaries exploit system behavior to extract sensitive information without triggering alerts. Majeed and Hwang (2023) demonstrated that synthetic data generated by AI can be used as background knowledge to analyze patterns in real or anonymized data and infer potentially private information. When applied to AI Note-taking tools, this raises significant concerns. Stored or generated transcripts from sensitive professional meetings could be exposed to privacy breaches, especially when shared across systems or used to train future AI models.

Gartner's 2025 prediction states that more than 40 percent of AI-related data breaches by 2027 will result from the improper use of generative AI. This forecast closely matches the risks described by Majeed and Hwang. One major contributing factor is the lack of transparency in how AI note-taking tools are integrated into virtual platforms. Tools such as Microsoft Copilot, Otter.ai, and Fireflies capture and process meeting data automatically. They may transfer that information across international regions and store it in third-party systems, often without the user's full awareness or explicit consent.

These findings show that synthetic data risks combined with unregulated use of AI note-taking tools can create serious cybersecurity threats in both personal and professional environments. This not only weakens the principles of informed consent and data transparency but also leads to long-term vulnerabilities in settings that involve confidential or sensitive information.

Our policy mapping revealed that none of the leading AI note-taker platforms fully enforce real-time, all-party consent: most rely on pre-meeting checkboxes or buried disclaimers. For example, our team utilized Fathom.ai and Google's NotebookLM in three of our weekly Zoom meetings. Both AI note takers provide incredible functionality, with Fathom.ai being able to join ongoing meetings directly and then record them in real time. Emailing participants a summary of the key points from the meeting or a full transcript of the meeting. With the ability to join meetings directly, no consent from meeting attendants are needed. This issue is shown in the flowchart in Figure 1 by Socradar. In contrast, NotebookLM takes a prerecorded transcript of the meeting then can output a summary of the meeting or create a flow chart of key takeaways from there. In NotebookLM's case, no consent from meeting attendees was needed outside of Zoom's own recording consent popup. Together, these findings validate our framework's emphasis on seamless consent prompts and carefully tuned alerts, while underscoring the need to balance security safeguards with user experience.


Initial Use of Notetaking App in a Client Call
Colleague uses app in meeting
Unintended Permission Granted via SSO
SSO login grants calendar access
Post-Meeting Summary Raises Questions
Summary email causes confusion
AI Notetaker Begins Joining Meetings Uninvited
App joins internal meetings
Discovery of Auto-Join Behavior
Realization of automatic meeting join

In conclusion, the results support the need for ethical guidelines, greater transparency, and stronger security protocols for AI note-taking tools. These steps are necessary to prevent future data breaches caused by improper use or lack of oversight.

5. Discussion

5.1 Interpretation of Results

The results of our research conclude that there are significant challenges when it comes to addressing privacy concerns with AI Note-taking. Cybersecurity risks are heightened since sensitive user data is attached to users of the note taking software. There are also issues due to the speed and intensity of the growth of AI in general. This means there are many unknowns that have yet to be addressed, leaving an abundance of room for adversaries to step in and attack user data.

There are limited laws on privacy policies as well. Laws for consent vary from state to state and in most cases, this is a developing topic. As leading AI software companies such as Fireflies.ai and Google sell user information and data to advertisers, it is often something that users are unaware of. Ethical AI designs must be produced proactively to ensure that users are given transparent information for what they are partaking in and the consequences that may follow. While companies are actively using ambiguous language in their policies, it is important to note that it is not an excuse for poor ethical responses. Just as it is unclear whether people must know if there is an AI Note-taker present in their meeting, however, it is also unclear if a company should be held responsible to ensure their users are educated on their policies to ensure informed consent.

5.2 Limitations and Lessons Learned

The ambiguity of legal terminology in privacy policies reviewed as well as the lack of a universal set of consent laws,makes it difficult to assign any one party accountability for the cybersecurity risks and user's education while using software such as AI Note-taking. Many privacy policies tend to have vague and unclear information regarding the kinds of information that will be collected, sold, used for AI model training, or for other uses. The internal handling of data is something that is kept fairly quiet which makes it challenging to analyze the true impact AI Note-taking has on the individual and broader security of those who may interact with such software. Generative AI, and by extension AI Note-takers, are essentially a black box with AI companies not wanting people to know exactly what goes on underneath the hood.

Despite how grey some areas of this topic may be, it is crystal clear that there are key elements to ensuring peak cybersecurity standards and critical information protection. Software systems such as AI Note-taking must remain transparent with users about the kinds of information that is shared and sold in terms the common person could understand so that sensitive information is less likely to be leaked to an adversary. It is essential that ethics are considered as AI Note-taking takes off in usage so that privacy, security, and consent are considered while developing these programs. Current laws are not developed enough to cover the topic at hand in depth so new standards and user guidelines must be added to this technology.

6. Conclusion and Future Work

6.1 Key Takeaways

Exploring how the adoption of Generative Artificial Intelligence has become more common in the daily life of individuals and companies, we were able to see that AI notetaking has been utilized and adopted too quickly due to its ability to efficiently summarize meetings and streamline information distribution in the workplace.

As shown by Google, Fireflies.ai, and Otter.ai's privacy policies, tech companies can obtain a vast amount of information that can then be stored for an indeterminate amount of time. With many of these companies not properly scrubbing the PII of the users before the information is sent off to either the US Government or third party actors that work with these AI companies. The lack of clear and concise user consent mechanisms is also problematic. Resulting in the possibility that many of these AI note-takers could be in breach of state level privacy laws within the US and the AI Consent Act if the data obtained by these AI is used to train the AI note-takers without the user's consent. One key risk that is shown in the Otter.ai legal case is that many AI notetakers capture every word spoken in a meeting—including sensitive or confidential information—and in some cases automatically share transcripts with all participants.

Studies have also shown that AI note-taking tools are vulnerable to attacks and exploits by adversaries. Making their relative cybersecurity questionable at best, woefully lacking at worst. While there are many benefits to using this tool, it does not seem to outweigh the risks associated with it. Data and user privacy, ethical concerns, and consent issues all play a valid and important role when determining the acceptance of AI note-takers despite its clear impact on cybersecurity risks and personal privacy problems.

As it is known that human error plays a major role in cybersecurity risks manifesting into something of substantial impact, it is vital that users are educated on the data that may be given up as a response to using a software. The ethics of making sure users are informed directly correspond to the cybersecurity risks and steps that can be taken to ensure strong security.

6.2 Potential Extensions and Impact

Future work would evolve our consent framework into a universal standard for AI Note-taker integration across all virtual-meeting platforms, ensuring each participant's preferences are honored in real time. For example, dynamic per-user consent prompts could appear before someone speaks and transcript segments with low model confidence could be automatically flagged as "Needs Review". This would guide moderators to verify content thereby maintaining both accuracy and trust between the users and AI note-takers. This would be done in conjunction with establishing clear guidelines for when and how these tools may be used, with explicit restrictions for sensitive or confidential discussions.

Modifications to the Cybersecurity Information Sharing Act (CISA) that inhibit the amount of Personally Identifiable Information (PII) not directly related to a cybersecurity threat that can be collected by tech companies alongside requiring tech companies to undergo rigorous scrubbing of user data before that data is sent to the US government. In addition to requiring any approved vendor to provide transparency on how data is stored, retained, and whether it is ever used for AI training.

Ethics Declaration: No ethical clearance was needed for this research.

AI Declaration: ChatGPT was used to determine what were the top AI Note-takers in June of 2025. Fathom.ai was used to record and provide notes from team meetings. NotebookLM was used to create meeting notes from team meeting recordings.

References

Allyn, B. (2025). *Class-action suit claims Otter AI secretly records private work conversations*. [online] Available at: https://www.npr.org/2025/08/15/g-s1-83087/otter-ai-transcription-class-action-lawsuit.

Bloomberg Government (2018). Transcript of Mark Zuckerberg's Senate hearing. *The Washington Post*. [online] 10 Apr. Available at: https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/.

Cadwalladr, C. and Graham-Harrison, E. (2018). *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*. [online] The Guardian. Available at: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

Domonoske, C. (2018). *Mark Zuckerberg Tells Senate: Election Security Is An 'Arms Race'*. [online] NPR.org. Available at: https://www.npr.org/sections/thetwo-way/2018/04/10/599808766/i-m-responsible-for-what-happens-at-facebook-mark-zuckerberg-will-tell-senate.

Drayton (2025). *If I Did It: How Meta Should Have Structured Its Non-Acquisition of Scale AI*. [online] Substack.com. Available at: https://enterprisevalue.substack.com/p/if-i-did-it [Accessed 29 Aug. 2025].

Espiner, T. and Jamali, L. (2025). Artificial intelligence: Disney and Universal sue Midjourney over copyright. *BBC*. [online] 12 Jun. Available at: https://www.bbc.com/news/articles/cg5vjqdm1ypo.

Fireflies.ai Corp. (2024). Available at: https://fireflies.ai/privacy_policy.pdf [Accessed 29 Aug. 2025].

Federal Trade Commission. "FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook." *Federal Trade Commission*, FTC, 24 July 2019, www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook.

Gartner (2025). Gartner Predicts 40% of AI Data Breaches Will Arise from Cross-Border GenAI Misuse by 2027. [online] Gartner. Available at: https://www.gartner.com/en/newsroom/press-releases/2025-02-17-gartner-predicts-forty-percent-of-ai-data-breaches-will-arise-from-cross-border-genai-misuse-by-2027.

Goel, S. and Webb, E. (2025). *Contractors see personal data when reviewing user chats with Meta's AI*. [online] Business Insider. Available at: https://www.businessinsider.com/meta-ai-chatbot-privacy-user-names-data-contractors-scale-alignerr-2025-8.

Google. (2024). *Privacy Policy – Privacy & Terms – Google*. [online] Available at: https://policies.google.com/privacy?hl=en-US#infosharing.

Herdiyanti, A. (2024). The Use of Automatic AI-based Notes and Transcription Services in Qualitative Research: Ethical and Methodological Concerns. *Proceedings of the ALISE Annual Conference*. [online] doi:https://doi.org/10.21900/j.alise.2024.1717.

Kukkonen, III C. and Tait, E. (2023). *Court Finds AI-Generated Work Is Not Copyrightable*. [online] Available at: https://www.jonesday.com/en/insights/2023/08/court-finds-aigenerated-work-not-copyrightable-for-failure-to-meet-human-authorship-requirementbut-questions-remain.

Lazzarotti, Joseph J. "AI Notetakers – Evaluating the Risks along with the Benefits." *Workplace Privacy, Data Management & Security Report*, 21 Mar. 2024, www.workplaceprivacyreport.com/2024/03/articles/artificial-intelligence/ai-notetakers-evaluating-the-risks-along-with-the-benefits/.

Majeed, A. and Hwang, S. O. (2024). *When AI Meets Information Privacy: The Adversarial Role of AI in Data Sharing Scenario*. [online] Available at: https://ieeexplore.ieee.org/document/10190078.

Otter.ai. (2024). *Otter.ai Privacy Policy | Otter.ai*. [online] Available at: https://otter.ai/privacy-policy.

SOCRadar® Cyber Intelligence Inc. (2025). *Your AI Notetaker Might Be a Liability: Insights from Stealer Logs - SOCRadar® Cyber Intelligence Inc.* [online] Available at: https://socradar.io/ai-notetaker-liability-insights-stealer-logs/ [Accessed 30 Aug. 2025].

Stone, D. LegalEagle (2025). *Disney Files Landmark Case Against AI Image Generator*. [online] YouTube. Available at: https://www.youtube.com/watch?v=zpcWv1lHU6I [Accessed 29 Aug. 2025].

Wikipedia. (2022). *DALL-E*. [online] Available at: https://en.wikipedia.org/wiki/DALL-E.

Wikipedia (2022). *Midjourney*. [online] Wikipedia. Available at: https://en.wikipedia.org/wiki/Midjourney.