The IP Practitioner's Guide for Advising the Next Generation of Startups

Image: Getty Images

Steve Maule and Michael Silliman

The last few years have thrown startups a whirlwind of challenges: a steep drop in venture capital investment,[1] a highly competitive marketplace,[2] the artificial intelligence (AI) revolution,[3] and an abundance of remote work.[4] Helping founders navigate this evolving landscape will require intellectual property (IP) practitioners to stay ahead of the curve. Our 2018 guide generally outlined the key steps IP practitioners need to take when working with startups.[5] Today's world requires revisiting these guidelines. It is critical that IP practitioners study these new risks and challenges to provide founders with legal advice tailored to the unique needs of startups.

Steve Maule is a senior associate at Baker Botts L.L.P. in Houston, Texas, where he focuses on high-tech patent litigation at the International Trade Commission and district courts. He also teaches as an adjunct law professor at the University of Houston Law Center. He can be reached at steve.maule@bakerbotts.com. **Michael Silliman** is special counsel at Baker Botts L.L.P. in Houston, Texas, where he advises startups and investors on IP matters, including tech transactions, portfolio management, counseling, and litigation. He can be reached at michael.silliman@bakerbotts.com.

Artificial Intelligence

Over 50% of companies are planning to incorporate AI technologies in 2024.[6] The AI and large language model (LLM) revolution has introduced both opportunities and challenges as startups leverage AI for innovation while grappling with the complexities of IP protection in this domain.[7] Despite the numerous and expanding legal implications of AI, the key issues for IP practitioners to address with startups include the patentability of AI-related inventions, AI-related risks and mitigation strategies, and the dangers of overreliance on AI for legal matters.

Patenting AI Inventions

As AI becomes a widely used technical tool, practitioners must familiarize themselves with the patentability of AI-assisted inventions. The U.S. Patent and Trademark Office (USPTO) has recently issued specific guidance on inventorship and subject matter eligibility of AI inventions, which practitioners should study to effectively navigate the complexities of patenting in this domain.[8]

USPTO's AI inventorship guidance. The AI inventorship guidance sets out the USPTO's interpretation of the inventorship requirements for AI-related inventions, aiming to strike a balance between incentivizing AI-assisted inventions without hindering future human innovation by locking up innovation created without human ingenuity.[9] According to the USPTO, AI-assisted inventions are not categorically unpatentable for improper inventorship, but a human must have contributed enough to be considered an inventor.[10] Accordingly, an AI-assisted invention is patentable in the U.S. only if a person "contributes significantly" to the invention.[11] Practitioners with AI-focused clients should analyze their client's technology to determine which aspects may be patentable under this guidance.

It is worth noting that the USPTO's AI-assisted inventorship guidance is not without controversy, as the guidance received criticism from both legal and industry representatives.[12] While the guidance has been effective since February 2024, the USPTO has actively sought comments on the guidance and has indicated that it plans to issue further guidance on AI.[13] Practitioners should monitor and stay abreast of further developments—from the courts and USPTO—about the patentability of AI-related inventions.

USPTO's AI subject matter eligibility guidance. The USPTO also recently issued updated guidance on subject matter eligibility that specifically focuses on AI inventions.[14] This guidance addresses eligibility of AI inventions and introduces three new examples designed to help examiners and stakeholders understand how to apply the subject matter eligibility criteria to AI inventions.[15] The guidance and examples focus on two steps in the subject matter eligibility analysis: (1) determining whether an AI claim recites a judicial exception (e.g., an abstract idea), and (2) evaluating if the AI invention integrates the judicial exception into a practical application by, for example, claiming a specific application of AI to a particular technological field (i.e., a particular solution to a problem).[16] Practitioners should consult this guidance in evaluating the patentability of a client's technology and in drafting claims that will pass muster at the USPTO.

Patentability of AI-assisted inventions outside of the U.S. Clients seeking patent protection outside of the U.S. will require an even more detailed analysis by practitioners, as requirements for AI-related inventions differ between jurisdictions. For example, the European Patent Office requires AI-related patent applications to include detailed disclosure of the aspects of the AI that bring about the technical effect provided by the invention (e.g., specific training data or a particular algorithm),[17] and the Japan Patent Office has indicated that it will require particular claim terminology and details regarding the function of the AI.[18] Startups with an international presence or plans to expand internationally will need careful advice on patenting of AI-related technology.

AI Risks and Mitigation Strategies

Advising startups on the use of AI involves a careful balance between embracing innovation and managing risk. We are in the nascent stages of AI disputes and litigation, which puts startups in the difficult position of reading about these risks in the news, without the guidance of any established best practices supported by case law. Additionally, that case law will likely take years to develop; meanwhile, the pace of AI development is on the order of weeks, and companies that avoid AI risk being left behind.

Instead of counseling wholesale against any AI use, it is incumbent on practitioners to help startups understand and mitigate risks. Many of the existing AI disputes are centered on the use of copyrighted training data.[19] If startups are using third-party AI tools and do not have control over the training of the AI, their risk will be largely based on their use of the AI outputs. These risks can be mitigated by ensuring that the startup has a strong indemnity for the use of the outputs from the AI vendor. Practitioners should review the indemnities available to the client for each AI tool and help them understand and negotiate the scope of their indemnity, if any. This may affect the startup's choice of AI tools, as indemnity offerings can vary considerably between vendors.

If companies are building an AI tool, or incorporating AI functionality into products, practitioners will need to do a deeper analysis of the AI tool itself. At a minimum, practitioners should identify whether the training data, the planned inputs of the tool,

THE KEY ISSUES FOR IP PRACTITIONERS TO ADDRESS WITH STARTUPS INCLUDE THE PATENTABILITY OF AI-RELATED INVENTIONS, AI-RELATED RISKS AND MITIGATION STRATEGIES, AND THE DANGERS OF OVERRELIANCE ON AI FOR LEGAL MATTERS.

and the generated outputs of the tool include confidential or copyrighted information of the startup or of third parties, and, if so, consider whether the tool could be modified to eliminate the presence of that information. Putting guardrails on how these tools are designed, trained, and used can significantly reduce the risk in their use, and provide defenses in any disputes down the road.

Indeed, guardrails and other AI policies are key areas where practitioners can provide value to their startup clients. Employees will inevitably seek out generative AI tools that make their job easier. Rather than prohibiting the use of these AI tools, practitioners should help founders create AI policies that establish guardrails, rules, and best practices for the use of AI. A comprehensive AI policy should address key questions such as: Which AI tools can be used? What types of data can be input into the LLM? How will the outputs of the LLM be used? Do these outputs need to be verified for accuracy and legal compliance? By establishing clear guidelines, practitioners can enable their clients to leverage the benefits of AI while minimizing potential risks.

Risks of Using LLMs for Legal Matters

In an effort to keep legal costs low, many founders are tempted to use LLMs to generate legal documents. It is hard to blame them—10 minutes with a publicly available LLM can spit out ostensibly accurate nondisclosure agreements (NDAs), supply agreements, joint development agreements, privacy policies, simple license agreements, and more. These specious documents may appear good enough for a startup on a shoestring budget with little desire to spend that on legal, but, without thorough vetting by an attorney, these documents are at best incomplete and at worst disastrous. Practitioners should warn founders of these risks and counsel them to resist the temptation to use publicly available LLMs for legal advice and document preparation without thorough review and verification by an attorney. For example, an ineffective NDA could jeopardize trade secret protection. Similarly, poorly drafted development, service, or license agreements could lead to costly contract disputes over IP ownership and licensing rights. This temptation can be tempered by offering founders templates for basic agreements and advising them of the risks of using an LLM for legal documents.

Founders may also be tempted to use LLMs for patent drafting. But confidential information like invention disclosures should not be entered into any publicly accessible LLM, as prompts are often stored and may even be used to train the LLM. Furthermore, like other legal documents, LLMs can generate specious patent applications. Practitioners should advise clients of the dangers of inputting confidential information into LLMs, as well as the legal nuances in patent drafting that will be missed by an LLM, risking the validity, enforceability, and scope of the patent.

That said, practitioners should consider whether private and patent-focused LLMs may have a place in provisional patent drafting, where the disclosure is largely a summary of the invention. Unlike public LLMs, some of these private LLMs do not store prompts or use inputs to train the model.[20] A suitably secure LLM from a reputable vendor could reduce the cost of an application. For example, an LLM could generate an initial draft, based on an inventor's notes or an invention disclosure form, for a practitioner to review and revise. However, practitioners should be cautious about the LLM tool they select and ensure that any client information will be kept confidential and not be used to train the tool.

Remote Work and Trade Secret Protection

Although remote work has always been more common in startups than in larger businesses, it has ramped up in startups following the outbreak of the COVID-19 pandemic.[21] This shift underscores the need for startups to ensure that their virtual work environments maintain robust trade secret protections. These protections are critical to maintaining enforceable trade secrets because a key element of trade secret misappropriation is that the information was actually protected as a trade secret.[22] To protect trade secrets in a remote work environment, startups should implement strict security policies and measures, such as encryption, secure access controls, and regular cybersecurity training for employees. Additionally, practitioners should advise startups to use robust NDAs, with both employees and third parties, to prevent unauthorized disclosure of sensitive information. Practitioners should help startups identify and protect these assets by developing comprehensive trade secret policies and recommending audits to ensure compliance. As discussed in our original 2018 guide, startups often overlook critical but less technical trade secrets, such as customer lists, operating procedures, and supplier lists.[23] Once identified, IP practitioners should counsel startups to distinguish and sequester trade secret information from nonproprietary information in their data management systems.

Open-Source Software

Open-source software (OSS) can be an attractive tool for startups, as it enables software developers to hit the ground running by building on the efforts of a community of developers and without dipping into limited financial reserves. Relying upon open-source technology can also be complementary to developing other IP, including patents and trade secrets.[24] Practitioners should help guide startups as to what IP protections are available and how those mesh with open-source technology.[25] And they should also caution founders that using OSS can open the door to a number of licensing and security risks.

OSS may be free of cost, but it is not free. Rather, it is typically released under one of numerous licenses and often imposes obligations on those using the OSS.[26] The first step to evaluating OSS is to identify and understand the corresponding license. For example, some "copyleft" licenses allow startups to modify the licensed software but include obligations that derivative works also be made available under the same license,[27] while permissive licenses merely ensure that the original OSS project remains publicly available.[28] Wikipedia (and likely other sites) may offer helpful comparisons of many open-source licenses,[29] but the wide variations in licenses necessitate that IP practitioners advise startups on the scope and specific contractual language in any OSS license.

Additionally, some OSS projects may include security vulnerabilities that risk exposing confidential information.[30] Some vulnerabilities are likely inadvertent, as OSS projects are often managed by small teams of volunteers.[31] However, attempts have been made to hijack OSS to introduce new security vulnerabilities.[32] Software audits may be one way to identify and address risks but can be costly.[33] Ultimately, OSS can be hugely valuable to startups (as well as established entities), but it is critical that IP practitioners advise startups to keep robust records of each OSS package used to limit the risk of legal disputes and track potential security vulnerabilities.

FTC Ban on Noncompetes

The FTC recently announced a new rule that would ban entering into and enforcing most noncompete agreements.[34] This rule, originally scheduled to go into effect in September 2024, is now in limbo following one decision upholding the rule in Pennsylvania and two decisions striking down the rule in Florida and Texas.[35] The FTC has appealed the Texas and Florida courts' decisions.[36] The FTC's rule may ultimately be headed to the U.S. Supreme Court,[37] but in the meantime, startups should be aware that noncompete rules of varying scope are already in effect in multiple states.[38]

Traditionally, noncompetes have been used to protect trade secrets and prevent employees from joining competitors for a limited period of time after leaving a company. The FTC proposes NDAs as alternatives to noncompete agreements. However, startups should be cautious, as overly strict NDAs could qualify as de facto noncompetes banned under the new FTC rule.[39] For example, an employment agreement could be unenforceable if it includes a confidentiality obligation that "has the effect of prohibiting the worker from seeking or accepting" other work.[40] A startup with this sort of language in its employment agreements could be placing its trade secrets in jeopardy.

With noncompetes potentially off the table and NDAs requiring careful review, startups must reevaluate both existing and future employment agreements and explore alternative methods for safeguarding their IP. For example, startups may consider more robust trade secret protections and recordkeeping; keeping a closer eye on departing and newly hired employees, and any information leaving or introduced with employees; and limiting access of trade secret information to only those employees with a true need to know.[41] In addition to being smart IP housekeeping tips, these are the tools that startups can use to protect critical IP wherever noncompete bans are in place.

To strike the right balance, employee NDAs should be specific and narrowly tailored to protect the most critical trade secrets. They should clearly define what constitutes confidential information and outline the obligations of employees regarding the protection and nondisclosure of such information. And startups may consider patents as safer alternatives to relying on NDAs to protect critical trade secrets. Practitioners should monitor the ongoing impact of and decisions addressing the FTC's rule, watch for guidance and case law regarding the scope of the FTC's de facto noncompete definition, and consider any relevant state-level noncompete rules that may be applicable.

WITH NONCOMPETES POTENTIALLY OFF THE TABLE AND NDAS REQUIRING CAREFUL REVIEW, STARTUPS MUST REEVALUATE BOTH EXISTING AND FUTURE EMPLOYMENT AGREEMENTS AND EXPLORE ALTERNATIVE METHODS FOR SAFEGUARDING THEIR IP.

Data Privacy

Client Base Considerations

Data privacy regulations, like Europe's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), are on the rise and require careful consideration.[42] Practitioners should ensure that startups consider numerous factors in their data collection practices such as: What kind of personally identifiable information (PII) is collected? Whose PII is collected? Where do these persons or entities reside? How do the startups plan to use this PII? And what are the ages of individuals whose PII is being collected?[43] These and other factors determine which statutes are in play. Privacy regulations may dictate individuals' rights in their information and implicate whether and how their data can be used to train AI systems.[44]

Data Policy and Contracts

In order to comply with these regulatory frameworks, startups should have comprehensive data policies in place that comply with the appropriate regulations. Practitioners should also caution startups that they may be held liable for any commitments to their clients, but transparent policies enable startups and customers alike to engage on agreeable terms.[45] These policies need to address data collection, storage, encryption, and sharing practices. Practitioners should ensure that agreements that may involve data transfers include the appropriate data privacy language (often seen in a data privacy addendum) to ensure compliance and mitigate legal risks.

Prosperous Startups Prefer Proficient IP Practitioners

Navigating the evolving landscape for startups will require IP practitioners to be flexible, proactive, and well-informed. By staying updated on the latest trends and regulatory changes, practitioners can provide valuable guidance to startups, helping them to protect their IP and achieve their business goals. ■

Endnotes

1. James Thorne, *Venture Fundraising May Not Recover until End of the Decade*, PitchBook (May 9, 2024), https://pitchbook.com/news/articles/venture-fundraising-forecast-quant (showing a 48% decline in venture capital fundraising between 2021 and 2024).

2. Economic News Release, U.S. Bureau of Lab. Stat., State Employment and Unemployment Summary (Oct. 22, 2024), https://www.bls.gov/news.release/laus.nr0.htm (showing 4% unemployment rate).

3. Mustafa Suleyman, *How the AI Revolution Will Reshape the World*, Time (Sept. 1, 2023), https://time.com/6310115/ai-revolution-reshape-the-world/.

4. Tim Smart, *Remote Work Has Radically Changed the Economy—and It's Here to Stay*, U.S. News (Jan. 25, 2024), https://www.usnews.com/news/economy/articles/2024-01-25/remote-work-has-radically-changed-the-economy-and-its-here-to-stay.

5. Natalie Alfaro Gonzales & Steve Maule, *The IP Practitioner's Guide to Working with Startups*, 10 Landslide, no. 6, July/Aug. 2018, at 7, https://www.americanbar.org/groups/intellectual_property_law/publications/landslide/2017-18/july-august/the-ip-practitioners-guide-working-startups/.

6. Anthony Cardillo, *How Many Companies Use AI?*, Exploding Topics (Aug. 21, 2024), https://explodingtopics.com/blog/companies-using-ai.

7. Although AI tools include LLMs (as well as numerous other tools supporting video, image, code generation, music creation, marketing, advertising, and voice synthesis), the term AI will be used in this article to refer to all flavors of AI technology.

8. Inventorship Guidance for AI-Assisted Inventions, 89 Fed. Reg. 10043, 10047–49 (Feb. 13, 2024); 2024 Guidance Update on Patent Subject Matter Eligibility, Including on Artificial Intelligence, 89 Fed. Reg. 58128 (July 17, 2024).

9. 89 Fed. Reg. at 10047.

10. *Id.* at 10045–49.

11. *Id.* at 10048.

12. *See, e.g.*, Hannah Albarazi, *USPTO's AI-Assisted Inventions Guidance Irks ABA IP Section*, Law360 (June 20, 2024), https://www.law360.com/articles/1846061/uspto-s-ai-assisted-inventions-guidance-irks-aba-ip-section.

13. 89 Fed. Reg. at 10045.

14. 89 Fed. Reg. at 58128, 58135–38.

15. *Id.*; *July 2024 Subject Matter Eligibility Examples*, U.S. Pat. & Trademark Off. (July 2024), https://www.uspto.gov/sites/default/files/documents/2024-AI-SMEUpdateExamples47-49.pdf.

16. 89 Fed. Reg. at 58134–38; *July 2024 Subject Matter Eligibility Examples*, *supra* note 15, at 5–35.

17. *See* European Pat. Off., Guidelines for Examination in the European Patent Office F-III-3, G-II, at 3.3.1 (2024), https://link.epo.org/web/legal/guidelines-epc/en-epc-guidelines-2024-hyperlinked.pdf. Unless readily apparent, the European Patent Office guidelines require a description of the technical effect of a machine learning algorithm by explanations, mathematical proof, experimental data, or the like. If the technical effect is dependent on particular characteristics of the training dataset used, those characteristics that are required to reproduce the technical effect must be disclosed. However, in general, there is no need to disclose the specific training dataset itself.

18. *See Newly Added Case Examples for AI-Related Technologies*, Japan Pat. Off. (Mar. 13, 2024), https://www.jpo.go.jp/e/system/laws/rule/guideline/patent/document/ai_jirei_e/jirei_add2024_e.pdf.

19. *See, e.g.*, Michael M. Grynbaum & Ryan Mac, *The Times Sues OpenAI and Microsoft over A.I. Use of Copyrighted Work*, N.Y. Times (Dec. 27, 2023), https://www.nytimes.com/2023/12/27/business/media/new-york-times-open-ai-microsoft-lawsuit.html; Complaint, N.Y. Times Co. v. Microsoft Corp., No. 2023-CV-11195 (S.D.N.Y. Dec. 27, 2023), 2023 WL 9750489.

20. *See, e.g.*, *Security*, DeepIP, https://www.deepip.ai/security (last visited Oct. 25, 2024).

21. *See, e.g.*, Sarah Lynch, *More Startups Embraced Remote Work in 2023*, Inc. (Apr. 2, 2024), https://www.inc.com/sarah-lynch-/more-startups-embraced-remote-work-in-2023.html.

22. *See, e.g.*, U.S. Pat. & Trademark Off., Intellectual Property Toolkit—Trade Secrets, https://www.uspto.gov/sites/default/files/documents/tradesecretsiptoolkit.pdf (last visited Oct. 25, 2024).

23. Gonzales & Maule, *supra* note 5.

24. *See, e.g.*, Ye Thu Aung, *Why Patents, Not Open Source? Do We Have to Choose One?*, LinkedIn (Apr. 7, 2022), https://www.linkedin.com/pulse/why-patents-open-source-do-we-have-choose-one-ye-thu-aung/.

25. *See id.*

26. *See, e.g.*, Peter Schneider, *Guide to the Total Cost of Ownership of Open-Source Software*, Qt Grp. (May 10, 2022), https://www.qt.io/blog/is-open-source-really-free.

27. *See, e.g.*, *What Is Copyleft?*, GNU, https://www.gnu.org/licenses/copyleft.en.html (last updated Jan. 2, 2022).

28. *See, e.g.*, *Exploring the MIT Open Source License: A Comprehensive Guide*, MIT Tech. Licensing Off., https://tlo.mit.edu/understand-ip/exploring-mit-open-source-license-comprehensive-guide (last visited Oct. 25, 2024).

29. *Comparison of Free and Open-Source Software Licenses*, Wikipedia, https://en.wikipedia.org/wiki/Comparison_of_free_and_open-source_software_licenses (last updated July 24, 2024).

30. *What Are Open Source Vulnerabilities?*, Sonatype, https://www.sonatype.com/resources/articles/what-are-open-source-vulnerabilities (last visited Oct. 25, 2024).

31. *See, e.g.*, Randall Munroe, *Dependency*, XKCD, https://xkcd.com/2347/ (last visited Oct. 25, 2024).

32. *See* Kelsey Piper, *A Hack Nearly Gained Access to Millions of Computers. Here's What We Should Learn from This*, Vox (Apr. 12, 2024), https://www.vox.com/future-perfect/24127433/linux-hack-cyberattack-computer-security-internet-open-source-software (describing efforts to infiltrate and introduce exploits into a widely used open-source tool).

33. *The Real Costs of a Software Audit*, SoftwareOne (Mar. 13, 2023), https://www.softwareone.com/en/blog/articles/2020/10/21/the-real-costs-of-a-software-audit.

34. Non-Compete Clause Rule, 89 Fed. Reg. 38342 (May 7, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/noncompete-rule.pdf.

35. Bryan Koenig, *FTC Fails 1st Test of Rulemaking Push in Noncompetes Loss*, Law360 (Aug. 21, 2024), https://www.law360.com/articles/1872097 (discussing the Texas court's conclusion that the FTC lacks "authority to create 'substantive rules regarding unfair methods of competition'"); Bryan Koenig, *FTC Powers Get a Boost in Philly in Noncompete Ban Saga*, Law360 (July 26, 2024), https://www.law360.com/articles/1861688 (discussing the Pennsylvania court conclusion that the FTC's proposed rule will "prevent unfair methods of competition in the form of non-compete agreements, both before they occur as well as after, to cease the past and ongoing harm they inflict"); Bryan Koenig, *Fla.'s The Villages Exempted from FTC Noncompete Ban*, Law360 (Aug. 15, 2024), https://www.law360.com/articles/1870230 (linking the Florida court's motion hearing characterizing the FTC's rule as "a hugely consequential expansion of regulatory authority" that "is not authorized").

36. Bryan Koenig, *FTC Appeals Noncompete Ban Loss to 5th Circ.*, Law360 (Oct. 18, 2024), https://www.law360.com/articles/1891731/ftc-appeals-noncompete-ban-loss-to-5th-circ-.

37. *See, e.g.*, Daniel A. Crane, *Predicting the Fate of the FTC's Non-Compete Ban*, Notice & Comment (Apr. 26, 2024), https://www.yalejreg.com/nc/predicting-the-fate-of-the-ftcs-non-compete-ban/.

38. Paul Starkman & Daniel Kinsella, *States Are Charting Their Own Course on Employment Noncompetes*, Bloomberg L. (Apr. 24, 2024), https://news.bloomberglaw.com/us-law-week/states-are-charting-their-own-course-on-employment-noncompetes; *State Noncompete Law Tracker*, Econ. Innovation Grp. (Oct. 11, 2024), https://eig.org/state-noncompete-map/.

39. 89 Fed. Reg. at 38361.

40. *Id.*

41. *See also* Meghan McCarty Carino, *How Companies Can Protect Trade Secrets Without Noncompete Clauses*, Marketplace (Apr. 25, 2024), https://www.marketplace.org/2024/04/25/how-companies-can-protect-trade-secrets-without-noncompete-clauses/ (suggesting alternatives to noncompete agreements may include "more onboarding sessions, bigger employee handbooks and tighter security, cyber and physical").

42. *See, e.g.*, *Which States Have Consumer Data Privacy Laws*, Bloomberg L. (Sept. 10, 2024), https://pro.bloomberglaw.com/insights/privacy/state-privacy-legislation-tracker/; *see also* Katrina Zhu, *The State of State AI Laws: 2023*, Elec. Privacy Info. Ctr. (Aug. 3, 2023), https://epic.org/the-state-of-state-ai-laws-2023/ (surveying "a surge in state AI laws proposed across the U.S.," many of which "are part of comprehensive consumer privacy laws").

43. *See, e.g.*, *California Consumer Privacy Act (CCPA)*, Cal. Dep't of Just. Off. of the Att'y Gen., https://oag.ca.gov/privacy/ccpa (last updated Mar. 13, 2024); Council Regulation 2016/679, 2016 O.J. (L 119) 1, https://eur-lex.europa.eu/eli/reg/2016/679/oj; Children's Online Privacy Protection Rule, 16 C.F.R. § 312; *see also* Andrew Chung, *US Supreme Court to Hear Challenge to Texas Age Verification for Online Porn*, Reuters (July 2, 2024), https://www.reuters.com/legal/us-supreme-court-hear-challenge-texas-age-verification-online-porn-2024-07-02/.

44. Chi Whitley, *How to Navigate Privacy and AI with a Customer-Centric Approach*, SOCi (Mar. 4, 2024), https://www.meetsoci.com/resources/blog/artificial-intelligence/ai-and-privacy/.

45. *See, e.g.*, *AI Companies: Uphold Your Privacy and Confidentiality Commitments*, Fed. Trade Comm'n (Jan. 9, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/01/ai-companies-uphold-your-privacy-confidentiality-commitments.