Q3/Q4 2024

WILSON SONSINI

AI/ML
ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

# ALL EYES ON AI: REGULATORY, LITIGATION, AND TRANSACTIONAL DEVELOPMENTS

## In This Issue



## President Trump Issues Executive Order on AI and Announces Private AI Fund

On January 23, 2025, President Donald J. Trump issued an executive order (EO), "Removing Barriers to American Leadership in Artificial Intelligence." The EO directs the Assistant to the President for Science and Technology (APST), the Special Advisor for AI and Crypto, and the Assistant to the President for National Security Affairs (APNSA), in coordination with others, to develop and submit to President Trump an action plan to sustain and enhance America's "global AI dominance."

The EO also directs the APST, the Special Advisor for AI and Crypto, and the APNSA to immediately review, in coordination with the heads of all agencies as they deem relevant, all policies, directives, regulations, orders, and other actions taken pursuant to former President Biden's executive order 14110 on artificial intelligence (AI), which was revoked by President Trump on January 20, 2025. If any actions are identified that are inconsistent with or present obstacles to President Trump's EO, then they will be suspended, revised, or rescinded in compliance with applicable law.

Just two days prior to issuing the EO, President Trump announced a private joint venture called Stargate during a White House briefing. According to President Trump, the joint venture will involve billions of dollars in private sector investment to build AI infrastructure in the United States.

## California Passes 17 AI Bills in 2024 Legislative Session

California's 2024 legislative session concluded with the passage of 17 bills covering the use and regulation of AI technology. Wilson Sonsini's client alert from October 10, 2024, discusses the most significant bills, and below is a catalog of the 17 bills. (See below entries for more substantive summaries of the most significant bills—SB 942 and AB 2013 (transparency), AB 3030

*Continued on page 2...*

## California Passes 17 AI Bills in 2024 Legislative Session *(Continued from page 1)*

(healthcare), and AB 1008 (California law updates)):

- *California Law Updates*
  - AB 1008: Amends the California Consumer Privacy Act's **definition of "personal information"** to include information in AI systems. See "AB 1008: California Adds Privacy Obligations for AI Model Developers" for more information.
  - AB 2885: Amends various laws to **harmonize their definitions of AI**. AI is defined as "an engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments."
- *Transparency*
  - SB 942: Requires covered providers to provide an **AI detection tool and disclosures** where content is AI-generated. See "SB 942: California's AI Transparency Act" for more information.

  - SB 896: Requires state agencies or departments that employ AI tools to directly communicate with individuals regarding **government services** to provide a disclaimer that the communication was AI-generated.
  - AB 2013: Requires developers of generative AI systems or services to disclose online a **summary of the datasets used to train the AI system** or service. See "AB 2013: California's New AI Training Data Transparency Law" for more information.
- *Healthcare*
  - AB 3030: Requires health facilities, clinics, physician's offices, and offices of a group practice to disclose the use of **AI to generate patient communications** pertaining to patient clinical information. See "AB 3030: California's New Law on AI in Health Care Services" below for more information.
  - SB 1120: Requires health care service plans and disability insurers that use **AI for utilization review and management decisions** to ensure adequate human oversight over AI-based determinations related to a patient's clinical history and circumstances.
- *Digital Likeness*
  - AB 1831 and SB 1381: Expand the scope of existing **child pornography** statutes to include matters digitally altered or generated using AI.
  - AB 1836: Prohibits the production or distribution of **digital replicas of a deceased personality's voice or likeness**, without prior consent, in an expressive audiovisual work or sound recording.
  - AB 2355: Requires committees that create, originally publish, or originally distribute **political advertisements** containing content altered using AI to include a specific disclosure regarding the use of AI.
  - AB 2602: Renders unenforceable contracts for the performance of personal or professional services involving the use of a **computer-generated copy of a person's voice or likeness** unless 1) the contract specifies the intended uses of the digital replica and 2) the person is represented by legal counsel or a labor union.
  - AB 2655: Requires large online platforms receiving reports of materially deceptive and digitally modified or created content related to **elections** to either remove the content or label that content during periods before and after an election.
  - AB 2839: Prohibits distribution of **election communications** containing media that has been digitally altered or manipulated in a deceptive way without disclosing the alteration/manipulation.
  - SB 926: Establishes the intentional creation and distribution of **sexually explicit images** that cause serious emotional distress as a misdemeanor.
  - SB 981: Requires social media platforms to provide mechanisms for reporting **sexually explicit digital identity theft**.

*Continued on page 3...*

## California Passes 17 AI Bills in 2024 Legislative Session *(Continued from page 2)*

- *Education*
  - **AB 2876**: Requires the California Instructional Quality Commission to consider including **AI literacy** into forthcoming curriculum frameworks.
  - **SB 1288**: Requires the Superintendent of Public Instruction to convene a working group to develop guidance for the **safe use of AI in education**.

In addition to signing these bills, California Governor Gavin Newsom vetoed SB 1047, which would have required developers of powerful AI systems to engage in pre-deployment safety testing and post-deployment monitoring. He noted in his veto message that the bill improperly focused on large models even though small ones could present similar risks, and did not consider whether an AI system deployed in high-risk environments engages in critical decision-making or uses sensitive data. Governor Newsom's veto represents a big win for the numerous industry members, politicians, and academics who lobbied against the bill, arguing that its passage would stifle AI innovation.

# SB 942: California's AI Transparency Act

On September 19, 2024, Governor Newsom signed SB 942, the California AI Transparency Act. The bill requires a person that creates, codes, or otherwise produces a generative artificial intelligence (GAI) system accessible in California (a "covered provider") that has over 1,000,000 monthly visitors or users to 1) offer a free and publicly available GAI detection tool, 2) provide public disclosures that content is GAI generated and 3) contractually obligate licensees of the GAI system to similarly provide such disclosures. The law will come into effect on January 1, 2026.

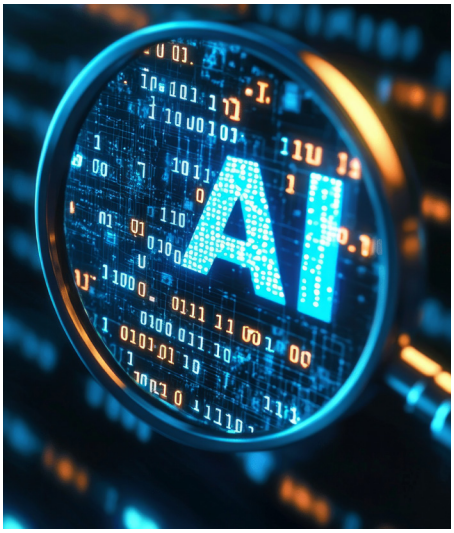
- *Obligations:*
  - AI Detection Tool: Covered providers are required to create a free, publicly accessible "AI detection tool" that allows users to assess whether content was created or altered by the covered provider's own GAI system. The AI detection tool must disclose any source data detected in the content without disclosing any personal source data. Users will be able to provide a URL or upload content directly to the AI detection tool. In addition, the AI detection tool must enable an API that allows users to use the tool from the covered provider's website. Finally, covered providers must collect user feedback of the AI detection tool and apply such feedback to improve the tool.
  - Disclosures that content is GAI generated: Covered providers must enable disclosures concerning 1) content created or altered by individuals using the covered provider's GAI system and 2) content generated by the covered provider's GAI system. Under the first category, covered providers must allow users to include a disclosure similar to watermarking, which is clear, easily understood to a reasonable person, and permanent or difficult to remove. Under the second category, the disclosure must include the name of the covered provider, the name and version of the GAI system, the time and date of the content's creation or alteration, and a unique identifier. In addition, the disclosure must be detectable by the covered provider's AI detection tool and be permanent or difficult to remove.
  - Contractual obligations for GAI licensees: Covered providers must contractually require a licensee of its GAI system to keep in place the disclosures discussed above. If a covered provider knows that a licensee is unable to provide such disclosures, then it must revoke its license within 96 hours.

- *Exemptions:* The law does not apply to providers of non-user-generated services, such as video games, television, streaming, movies, or interactive experiences.
- *Enforcement:* The Attorney General, a city attorney, or a county counsel have enforcement authority for violations of the act and can seek $5,000 per violation. If a licensee violates its contractual obligations, enforcement can include injunctive relief and reasonable attorney's costs and fees.

# AB 2013: California's New AI Training Data Transparency Law

On September 28, 2024, Governor Newsom signed AB 2013, which requires developers of generative artificial intelligence (GAI) systems or services to post documentation online regarding the data used to train the system or service. Under this bill, GAI includes "artificial intelligence that can generate derived synthetic content, such as text, images, video, and audio, that emulates the structure and characteristics of the artificial intelligence's training data."

- *Obligations:* The necessary disclosures include a high-level summary of the datasets used to develop the GAI systems or services, including: the sources or owners of the datasets; a description of how the datasets further the intended purpose of the AI system or service; the number of data points included in the datasets; a description of the types of data points within the datasets; whether the datasets include any data protected by copyright, trademark, or patent, or whether the datasets are entirely in the public domain; whether the datasets were purchased or licensed by the developer; whether the datasets include personal information as defined by the California Consumer Privacy Act (CCPA); whether the datasets include aggregate consumer information as defined by the CCPA; whether there was any cleaning, processing, or other modification to the datasets by the developer; the time period during which the data in the datasets were collected, including a notice if the data collection is ongoing; the dates the datasets were first used during the development of the GAI system or service; and whether the GAI system or service used or continuously uses synthetic data generation in its development.




- *Exemptions:* The bill exempts developers from the disclosure requirements in three circumstances: 1) when the GAI system or service's sole purpose is to help ensure security and integrity; 2) when the GAI system or service's sole purpose is the operation of aircraft in national airspace; and 3) when the GAI system or service was developed for national security, military or defense purposes and is made available only to a federal entity.
- *Effective Date:* The disclosure requirements apply to a GAI system or service released on or after January 1, 2022. Such disclosures must be made on or before January 1, 2026. Thereafter, such disclosures apply to any GAI system or service, or a substantial modification to a GAI system or service, that is made publicly available to Californians for use.

# AB 3030: California's New Law on AI in Healthcare Services

On September 28, 2024, Governor Newsom signed AB 3030, which concerns new disclosure requirements for certain uses of GAI in healthcare services. The law covers healthcare facilities, clinics, physician's offices, or the office of a group practice that uses GAI to generate written or verbal patient communications concerning "patient clinical information" (i.e., information relating to the health status of a patient). The law expressly recognizes that administrative matters, such as appointment scheduling and billing, are not covered.

- *Obligations:* Covered healthcare services must provide a disclaimer to the patient that the relevant communication was generated by GAI. The disclosure requirements vary by type and manner of communication (see below). In addition to these disclosure requirements, covered healthcare services must provide clear instructions explaining how a patient could contact a human healthcare provider, employee of the health facility, clinic, physician's office, or the office of the group provider.

*Continued on page 5...*

## AB 3030: California's New Law on AI in Healthcare Services *(Continued from page 4)*

| Type of Communication | Required Disclosure |
|---|---|
| Written communications involving physical and digital media (e.g., letters and emails) | The disclaimer must appear prominently at the beginning of each communication. |
| Written communications involving continuous online interactions (e.g., chat-based telehealth) | The disclaimer must be prominently displayed throughout the interaction. |
| Audio communications | The disclaimer must be provided verbally at the start and end of the interaction. |
| Video communications | The disclaimer must be prominently displayed throughout the interaction. |

- *Exemptions:* AB 3030 does not cover all communications generated by GAI. Notably, communications generated by GAI that are read and reviewed by a human licensed or certified healthcare provider need not contain the required disclosures.
- *Enforcement:* Enforcement of violations varies by category of healthcare service. The Medical Board of California or the Osteopathic Medical Board of California have jurisdiction over violations by physicians. Licensed health facilities and licensed clinics are subject to the enforcement mechanisms described in Article 3 Chapters 2 and 1, respectively, of the California Health and Safety Code.

# AB 1008: California Adds Privacy Obligations for AI Model Developers


On September 28, 2024, Governor Newsom signed AB 1008 into law, which introduces new privacy obligations for personal information in AI systems. The bill amends the California Consumer Privacy Act (CCPA)'s definition of "personal information" to include information contained in "abstract digital formats," specifically including "artificial intelligence systems that are capable of outputting personal information."

The amendment clarifies that the CCPA's privacy obligations cover personal information regardless of format. AI systems capable of outputting personal information may be covered by CCPA, and consumers may assert privacy rights to the output of AI models involving their personal information. Moving forward, AI model developers may be required under the CCPA to respond to consumer requests regarding the access, deletion, correction, sharing, and sale of personal information. With these new privacy obligations, AI model developers should consider several paths towards compliance, including:

1) at the input stage: training models without using personal information and relying instead on properly de-identified information;

2) at the training stage: implementing "un-learning" mechanisms to retroactively remove personal information from being used as training data by AI models; and

3) at the output stage: implementing output suppression mechanisms to prevent personal information from being generated by AI models.

# U.S., UK, and EU (Among Others) Sign First International AI Safety Treaty

In September 2024, several countries, including the U.S., UK, and EU, signed the Council of Europe's Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law (the "Framework"). This Framework is the first multilateral treaty focused on AI.

The Framework was developed by the Council of Europe to ensure the stability and inalienability of human rights, democracy, and law in the face of the various risks posed by AI. These risks include privacy breaches, the spread of misinformation through false information from AI, and the use of biased data, as well as detrimental effects on human health, the environment, and employment. Countries that sign this treaty are committing to implement various enumerated principles related to the AI lifecycle management to help combat these risks.

The Framework will enter into force on the first day of the month, three months after five signatories, including at least three Council of Europe member states, have ratified it; the ratification process comes after the Framework has been signed.

---

# EU Privacy Regulators Confirm That Legitimate Interest Can Be a Valid Legal Basis for AI Model Training and Deployment

The European Data Protection Board (EDPB), which is formed by the data protection authorities of all EU countries, issued an opinion on December 17, 2024, addressing the use of legitimate interest as a legal basis for training and deploying AI models. The EDPB confirms that organizations can, in principle, rely on legitimate interest under the General Data Protection Regulation (GDPR) for processing non-sensitive personal data in the AI context if they implement certain safeguards.

These safeguards may include measures that facilitate the exercise of individuals' rights, and enhanced transparency measures that go beyond disclosures in a privacy policy. Other technical measures, such as respecting robots.txt signals when collecting publicly available data are also key. Additionally, conducting Data Protection Impact Assessments (DPIAs) can help identify and mitigate risks associated with AI processing. Companies should also establish mechanisms for data subjects to easily exercise their rights, such as access, rectification, and objection to data processing.

The EDPB also clarified the circumstances under which AI models may be considered anonymous or not. The EDPB found that an AI model is anonymous—and thus no longer subject to the GDPR—if the likelihood of either i) direct (including probabilistic) extraction of personal data used to train the model or ii) of obtaining, intentionally or not, such personal data from queries, is insignificant. The following safeguards help to argue that a model is anonymous: limiting the collection of personal data to train the model (e.g., including pseudonymizing or filtering personal data) before the training begins; privacy-preserving techniques during model training (e.g., differential privacy); measures to prevent the model from including personal data in the output; document-based audits; and robust testing.

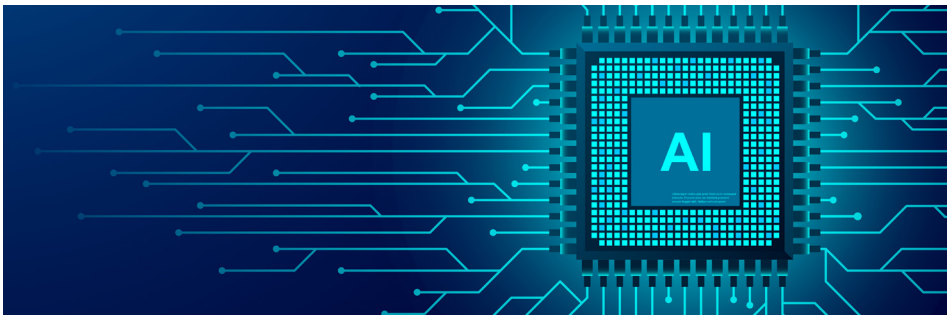
In summary, while legitimate interest can serve as a legal basis for processing non-sensitive personal data in AI model training and deployment, organizations must conduct thorough assessments, maintain transparency, and implement robust safeguards to ensure compliance with GDPR requirements.

For additional information, please see our recent Client Alert.

# EU AI Act Developments

*The EU AI Act is in effect.* As of February 2, 2025, certain AI systems which are deemed to pose an unacceptable risk are prohibited in the EU. In addition, companies need to ensure their staff understand the risks and requirements of using AI. To help companies and regulators apply the AI Act consistently, the European Commission (EC) is preparing guidelines on the definition of an "AI system" as well as guidelines on prohibited AI practices. On February 4, 2025, the EC issued a draft version of its guidelines on prohibited AI. For more information on the scope and requirements of the AI Act, please see our 10 Things You Should Know About the EU AI Act.

*Third draft of the General-Purpose AI Code of Practice is expected*. The EC is also tasked with preparing the General-Purpose AI Code of Practice (Code). A second draft of the Code was published on December 19, 2024, based on feedback received from the first draft of the Code which was published on November 14, 2024. The Code guides how companies can comply with the AI Act's requirements for general-purpose AI (GPAI). There has been considerable




interest from stakeholders, and the second draft of the Code was informed by the content discussed at working group meetings (further details of the working groups involved with the drafting process are available here). A third draft is expected in the coming weeks, and the Code is expected to be finalized by May 2025.

*Oversight and enforcement structures are being established.* The AI Act will be enforced by the EC (in relation to GPAI models) and national authorities. EU countries have until August 2, 2025, to appoint the competent national authorities. Some countries have already begun appointing the competent authorities. For instance, Spain established a new dedicated AI agency (the Spanish AI Supervisory Agency). In addition, the EC is establishing a new scientific advisory group for AI. Also, the EU AI Board, which advises the EU has held two meetings since its inception on August 1, 2024. In the first meeting on September 10, 2024, the AI Board discussed EU AI policy, EC guidance on the AI Act's implementation and best practices for national approaches to AI governance and AI Act implementation. In its second meeting on December 10, 2024, they adopted their Terms of Reference, discussed AI literacy in the EU, reviewed updates to the risk management framework of the Council of Europe Committee on AI, and observed the progress of the Code of Practice for general-purpose AI.

# EU and UK Data Protection Authorities Are Monitoring Use of Personal Data to Train AI

Data Protection Authorities across Europe are closely monitoring how providers of AI are using personal data of individuals located in the EU/UK to train their generative AI models. On September 4, 2024, the Irish Data Protection Commission (IDPC) announced that X had agreed to cease processing personal data of individuals located in the EU on a permanent basis. In the UK, the Information Commissioner's Office (ICO) announced on September 20, 2024, that a large social media company had suspended its model training pending further engagement with the ICO. This followed an ICO announcement from earlier the same month, that Meta had resumed training generative AI using user Facebook and Instagram user data, after it paused training in response to a request from the ICO in June 2024. The ICO emphasized that it is monitoring Meta's compliance.

## Below-Threshold Merger Review for AI Partnerships

On September 3, 2024, the European Court of Justice (ECJ) issued a judgment in the *Illumina/Grail* case holding that the European Commission (EC) may not accept merger review referrals filed by Member States that are not competent to review that transaction under their own national rules (a policy which had enabled the EC to review so-called "killer acquisitions" of small, innovative companies). Following the ECJ's judgment, multiple European antitrust authorities continued to speak up in favor of introducing special powers to review at least some below-threshold mergers.

On November 27, 2024, Andreas Mundt, President of Germany's Federal Cartel Office (FCO), stated in an interview that the FCO will ask German lawmakers to change German merger control thresholds to include a company's "possible or future" activities in Germany and to also lower the transaction value criteria from €400 million (US$421 million) to €300 million (US$315 million), expressly noting that it "would be a good result" if the changes succeeded in catching AI partnerships. Germany intends to update its competition rules in 2025.

## Updates on Treatment of AI Partnerships in Europe Under Merger Rules

European antitrust authorities continue to show great interest in AI partnerships and have reviewed several under merger rules or are at least attempting to do so. In some cases, antitrust authorities have come to the conclusion that the conditions (e.g., provision of compute, observer members on the board, non-exclusive licenses) of the specific AI partnership did not result in one company gaining control over the other and as such was not deemed a merger, with different standards across jurisdictions. In other cases, the AI partnership—while being deemed a merger—did not meet the local turnover thresholds required under merger control rules. While some antitrust authorities in Europe are already able to call in below-threshold mergers, others are considering changing their merger control regimes in order to be able to review AI partnerships (see above, *Below-Threshold Merger Review for AI Partnerships*).

On September 18, 2024, the EC announced it would not review the acquisition of certain assets of Inflection AI by Microsoft, after all Member States who had requested a referral of the matter to the EC withdrew their requests (following the September 3, 2024, *Illumina* judgment, which held that Member States cannot refer a transaction to the EC if their own national thresholds are not met). The EC noted that as part of the transaction, Microsoft had agreed to hire two co-founders of Inflection, made employment offers to most of Inflection's employees, and had received a non-exclusive license for Inflection's intellectual property and a waiver of any legal rights by Inflection for hiring its staff. The EC considered that the transaction included all assets necessary to transfer Inflection's position in the markets for generative AI models and AI chatbots to Microsoft. The EC noted its belief that this transaction amounted to a concentration reviewable in principle under the EU Merger Regulation (EUMR). Microsoft notified the transaction under Article 14 of the Digital Markets Act, noting that it believed the transaction did not amount to a concentration reviewable in principle under the EUMR.

On November 29, 2024, Germany's FCO announced that it would not review the acquisition of certain assets of Inflection AI by Microsoft. While the FCO believed that the arrangements between Microsoft and Inflection AI constituted a merger which would be in principle reviewable under German law, it concluded that Inflection AI did not have the "substantial operations" in Germany necessary to reach the merger review thresholds, with too few local users of Inflection AI's Pi chatbot.

*Continued on page 9...*

### Updates on Treatment of AI Partnerships in Europe Under Merger Rules *(Continued from page 8)*

On September 27, 2024, the UK's Competition and Markets Authority (CMA) announced that Amazon's partnership with Anthropic had not resulted in a relevant merger situation and closed its merger investigation. The full decision, published on October 17, 2024, clarified that Anthropic's UK turnover did not exceed £70 million and that both parties together did not meet the share of supply test for any goods or services. The CMA did not take a position on whether Amazon's investment of US$4 billion, in connection with several non-exclusive agreements and consultation rights, could have led to an exercise of material influence over Anthropic.

On November 19, 2024, the CMA announced it had closed its investigation into Google's partnership with Anthropic as it also did not result in a relevant merger situation. The CMA did not believe that Google could exercise material influence over Anthropic as a result of the partnership. In addition, the CMA found that Anthropic's UK turnover did not exceed the £70 million threshold, but it did not reach a conclusion on the share of supply test.

## Market Studies and White Papers Addressing AI

On September 19, 2024, the EC published a policy brief on competition in generative AI and virtual worlds following two calls for contributions from January 2024. The policy brief highlighted the EC's concerns about competitive challenges from the vertical integration of large tech platforms in the generative AI space but acknowledged that their partnerships with smaller developers of AI models could have procompetitive effects.

On September 27, 2024, the Portuguese Competition Authority (AdC) published a paper on accessing and using data in generative AI. The AdC identified that AI model developers were shifting from using publicly available data to licensed proprietary data, which could create barriers to entry and may reinforce market power. The AdC stated that data exclusivity and preferential access could potentially infringe competition law. On December 4, 2024, the AdC published an additional paper on model openness in generative AI. The AdC spoke in favor of open models but warned about the risk of open models becoming closed later, potentially locking in third-party developers.

## U.S. Revises DOJ's Evaluation of Corporate Compliance Programs

On September 23, 2024, Principal Deputy Assistant Attorney General Nicole M. Argentieri announced the latest revision of the U.S. Department of Justice's Evaluation of Corporate Compliance Programs (the ECCP), a document meant to assist prosecutors in analyzing the efficacy of corporate compliance programs and to help companies understand the DOJ's expectations for their compliance programs. The revision contains several key updates aimed at addressing potential AI misuse and encouraging companies to adapt their compliance policies in light of AI advances.

The DOJ explicitly approved companies' use of AI in their compliance programs. The changes to the ECCP make it clear that the DOJ recognizes that as businesses change how they operate, compliance also has to change if it is going to be effective. Per the revised ECCP, companies using AI should update their compliance policies to better identify and manage potential risks posed by the developing technology. The ECCP asks 10 new questions to help guide companies crafting these policies, factoring in the speed at which a company can detect and correct decisions made by AI that

*Continued on page 10...*

## U.S. Revises DOJ's Evaluation of Corporate Compliance Programs *(Continued from page 9)*

are inconsistent with the company's values, along with whether the company has procedures in place to curb potential negative or unintended consequences resulting from AI usage. Companies are also advised by the ECCP to account for AI in their risk assessments and develop controls to ensure that AI is used only for its intended purposes.

The revised compliance guidelines are an important step in the U.S. government's effort to adapt existing recommendations to better address new and emerging technologies, and they may have significant implications for a broad swath of technology companies.

# New U.S. "Outbound" Investment Rules Will Upend Diligence for AI-Related Transactions

On October 28, 2024, the U.S. Treasury Department (Treasury) issued its final rules on "outbound" U.S. investment (the Outbound Rules)—i.e., investments by *U.S.* persons in *foreign* entities, the opposite posture of investments currently subject to the jurisdiction of the Committee on Foreign Investment in the United States (CFIUS). The new rules, which went into effect on January 2, 2025, implement the Outbound Investment Security Program mandated by former President Biden's August 9, 2023, Executive Order (Outbound Order). While President Trump has not rescinded the Outbound Order or the new rules, he has ordered a review of both documents. While this review is pending however, they will remain in effect.


The new rules create incentives for U.S. persons and entities—and some non-U.S. persons and entities—to engage in diligence and obtain representations across a broad range of transactions, including those involving AI systems and related technologies. Specifically, the Outbound Rules either prohibit or require notification of certain investment activities by U.S. persons (including their foreign subsidiaries) involving target companies that are related to the People's Republic of China (the PRC). For an investment to be subject to the rules, those PRC-related companies must work on specific sub-sets of national security technologies and products—namely, semiconductors and microelectronics; quantum information technology; and certain AI systems (discussed further below). However, unlike the CFIUS review process, the Outbound Rules do not establish a case-by-case review and clearance regime. Instead, U.S. persons are responsible for conducting "a reasonable and diligent inquiry"—which, under the rules, can include both seeking information and obtaining contractual assurances—to ensure that any given transaction is not restricted by the new regime. U.S. persons are also required to take "all reasonable steps to prohibit and prevent" a controlled foreign entity from engaging in a prohibited transaction.

If a U.S. person knew or should have known that an investment into an AI or other company would trigger the Outbound Rules, they can be held liable for violations, which may result in civil or criminal penalties and/or a forced divestiture. Accordingly, U.S. persons should conduct thorough diligence before engaging in transactions that may be prohibited or notifiable under the new regime.

*Continued on page 11...*

## New U.S. "Outbound" Investment Rules . . . *(Continued from page 10)*

To determine whether the Outbound Rules apply to a given transaction, parties should consider the following five-part conjunctive test:

1. **Does the transaction involve a "U.S. person"?** The set of U.S. persons is broadly defined to include U.S. citizens (wherever located), lawful permanent residents, entities organized under U.S. laws, and individuals physically present in the U.S., regardless of nationality. Foreign subsidiaries of U.S. persons are also separately covered by the rules—their U.S. parents are required to ensure their compliance.

2. **Is the U.S. person engaging in a type of transaction covered by the rule?** The set of covered transactions includes i) acquiring equity or "contingent equity" (such as convertible notes); ii) making a loan or providing other debt financing that is either convertible or affords the right to be involved in the target's management in certain capacities; iii) converting contingent equity; iv) acquiring, leasing, or developing property or assets in the PRC; v) forming a joint venture; or vi) obtaining a limited partner or equivalent stake in an investment vehicle.

3. **Is the target of the transaction engaged in a "covered activity"?** As noted below, this includes working on semiconductors, quantum information technology, or AI that is useful in certain sectors or has certain capabilities.

4. **Does the target have the requisite ties to a "country of concern" (the "China Ties Criteria")?** For the purposes of the Outbound Rules, a "country of concern" is defined as the PRC, including the Special Administrative Regions of Hong Kong and Macau. The China Ties Criteria includes not only entities based in or incorporated under Chinese law, but also businesses with less obvious links to the PRC—e.g., those with significant direct or indirect PRC ownership or businesses with investments in the PRC that are material to their bottom line. In addition, indirect investments into PRC-related businesses are covered by the rules, and so a non-PRC target's downstream activities and investments should also be evaluated for PRC connections.

5. **Is the transaction an "excepted transaction"?** Exemptions include, among others, investments in publicly traded securities, certain limited partner (LP) investments of $2 million or less or where the LP has obtained certain contractual assurances, derivatives, or certain intracompany transactions between U.S. parent firms and controlled foreign entities. The Outbound Rules also allow a U.S. person to seek an exemption from the application of the restrictions on the basis that a transaction is in the national interest of the United States.

At first glance, this five-part test appears relatively narrow and straightforward to meet: a transaction must satisfy all five tests in order to be covered by the Outbound Rules. Indeed, Treasury noted in the implementing order that the rules are intended to be "narrowly scoped to focus on a limited subset of investment activity" to "avoid unintended impacts in broader sectors of the U.S. or global economies."

In practice, however, the Outbound Rules create new diligence obligations *across a broad swath of technology transactions, particularly those involving AI systems or related technologies.* As illustrated by the table below, the scope of the subcategories spans multiple industries that could implicate AI, and the China Ties Criteria may not be self-evident in a given transaction. For example, a U.S. fund looking to invest in a robotics company headquartered in San Francisco or Tokyo may unwittingly find the transaction subject to the Outbound Rules if the robotics company is engaged in a covered activity **and** has the requisite direct or indirect ties to China—e.g., through a subsidiary or through high levels of Chinese ownership in the parent. Accordingly, even parties to U.S.-to-U.S. transactions need to perform reasonable diligence, including securing binding commitments, to ensure compliance with the Outbound Rules (i.e., to satisfy the requisite knowledge standard) and avoid incurring liability.

Failure to comply with the new regime may result in severe consequences, including both civil and criminal penalties and forced divestment. Violations of the new rules may result in civil penalties of up to $250,000 or twice the value of the transaction, whichever is greater, while willful violations could lead to criminal penalties, including fines of up to $1 million and/or imprisonment for up to 20 years. Treasury also has the authority to nullify, void, or compel the divestment of certain prohibited transactions.

*Continued on page 12...*

## New U.S. "Outbound" Investment Rules . . . *(Continued from page 11)*

| Covered Products and Technologies | Notifiable Transactions | Prohibited Transactions |
|---|---|---|
| AI-system means:<br>a) A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments—i.e., a system that:<br>1) uses data inputs to perceive real and virtual environments;<br>2) abstracts such perceptions into models through automated or algorithmic statistical analysis; and<br>3) uses model inference to make a classification, prediction, recommendation, or decision.<br>b) Any data system, software, hardware, application, tool, or utility that operates in whole or in part using a system described in (a). | Covered transactions related to the development of any AI system that is:<br>• Designed, but not exclusively, for military, government intelligence, or mass surveillance end uses.<br>• Intended by the target to be used in cybersecurity applications, digital forensics tools, penetration testing tools, or the control of robotic systems.<br>• Trained using a quantity of threshold of computing power greater than 10^ 23 computational operations. | Covered transactions related to the development of any AI system that is:<br>• Designed or intended to be used *exclusively* for military, government intelligence, or mass surveillance end use.<br>• Trained using a quantity of computing power greater than 10^25 computational operations generally or trained using primarily biological sequence data and a quantity of computing power greater than 10^24 computational operations using primarily biological sequence data. |
| For the purposes of the quantum information technologies category, "quantum computer" means:<br>A computer that performs computations that harness the collective properties of quantum states, such as superposition, interference, or entanglement. | N/A: All quantum-related activity covered by the Outbound Rules is prohibited. | Covered transactions related to the:<br>• Development, installation, sale, or production of any supercomputer enabled by advanced integrated circuits that can provide a theoretical compute capacity of 100 or more double-precision (64-bit) petaflops or 200 or more single-precision (32-bit) petaflops of processing power within a 41,600 cubic foot or smaller envelope.<br>• Development of a quantum computer or producing any of the critical components required to produce a quantum computer.<br>• Development or production of a quantum sensing platform designed or intended to be used for military, government intelligence, or mass surveillance end use.<br>• Development or production of any quantum network or quantum communication system designed or intended to be used for: 1) networking to scale up the capabilities of quantum computers; 2) secure communications; or 3) any other application that has military, government intelligence, or mass surveillance end use. |

*Continued on page 13...*

## New U.S. "Outbound" Investment Rules . . . *(Continued from page 12)*

| Covered Products and Technologies | Notifiable Transactions | Prohibited Transactions |
|---|---|---|
| Semiconductors and microelectronics | Covered transactions related to the design, fabrication, or packaging of integrated circuits not otherwise covered by the prohibited transaction definition are subject to a notification requirement. | Covered transactions related to the:<br>· Development or production of any electronic design automation software for the design of integrated circuits or advanced packaging.<br>· Development or production of front-end semiconductor fabrication equipment designed for performing the volume fabrication of integrated circuits, equipment for performing volume advanced packaging, or other items designed exclusively for use in or with extreme ultraviolet lithography fabrication equipment.<br>· Design of any integrated circuits that meet or exceed the performance parameters in Export Control Classification Number 3A090.a, or integrated circuits designed for operation at or below 4.5 Kelvin.<br>· Fabrication of certain integrated circuits.<br>· Packaging of integrated circuits using advanced packaging techniques. |

For additional information about these new outbound investment rules, please see our recent Client Alert.

# Copyright Office Issues Report on Copyrightability of AI-Generated Works

On January 29, 2025, the United States Copyright Office (the Copyright Office) issued guidance clarifying its view of the copyrightability of AI-generated works. The document is the second part of the Copyright Office's report on Copyright and Artificial Intelligence; the first part was issued in July 2024 and covered copyright concerns raised by digital replicas created by AI. This second part establishes the Office's view that the existing framework of copyright law is sufficient to address the copyrightability of AI-generated works; that AI systems fit within that framework as tools to be used by authors; and that AI-generated works may be copyrightable, subject to evaluation on a case-by-case basis.

In issuing the report's second part, the Copyright Office did not recommend any new legislation. The Copyright Office instead offered its analysis within the existing framework of copyright law. The Copyright Office compared "AI systems" (which it defines in its Notice of Inquiry issued in August 2023) to tools to be used by authors, similar to how authors may use cameras to create copyrightable photographs. In drawing this comparison, the Copyright Office reaffirmed its stance that an AI system itself cannot be an "author" (a required element of copyrightability).

The Copyright Office also emphasized that for AI-generated works to be copyrightable, they must contain a sufficient level of human creativity. Just as the copyrightability of photographs may hinge on a certain level of human decision-making to determine framing, lighting, and angle, the Copyright Office said the use of AI systems requires a certain level of human creativity for the result to be copyrightable. The Copyright Office concluded that the mere submission of a prompt to an

*Continued on page 14...*

## Copyright Office Issues Report on Copyrightability of AI-Generated Works *(Continued from page 13)*

AI system does not make the output copyrightable—"prompts do not alone provide sufficient control" to make a work copyrightable. Rather, that prompt, or some other input to the resulting work, must itself involve sufficient human creative input. Simple or generic prompts are unlikely to meet the threshold for creativity, and are thus, according to the Copyright Office, unlikely to result in copyrightable outputs from the AI system.

While the Copyright Office's guidance does not establish new law (and is not


binding on courts), it does provide clarity to companies using AI systems to generate potentially copyrightable outputs, since courts often consider the Copyright Office's policies and interpretations as persuasive authority, especially in cases posing novel questions of copyright law. Companies should thus heed the guidance in the report when considering their usage of AI systems, especially as it relates to works that companies may want to protect under copyright law.

# Copyright Office Rejects Anti-Circumvention Exception for AI Research


On October 28, 2024, the U.S. Copyright Office issued a final rule in which it rejected a petition that would have exempted certain generative AI-related research on AI model bias from the Digital Millennium Copyright Act's (DMCA's) prohibitions on circumvention. This petition was one of the proposals the Copyright Office referenced in its October 2023 notice of proposed rulemaking (NPRM); in that NPRM the Copyright Office indicated that it had received proposals for seven new classes of exemptions from the DMCA's anti-circumvention provision.

Section 1201 of the DMCA prohibits circumvention of "technological measures" (often referred to as "technological protective measures" or "TPMs") that control access to copyright-protected works. This protection extends to copyright-protected aspects of AI systems, meaning that anyone who bypasses TPMs of AI systems without authorization may be subject to copyright-related claims and even criminal charges.

The final rule issued by the Copyright Office explained that the Register of Copyrights found that "the adverse effects identified by proponents [of the exemption] arise from third-party control of online platforms rather than the operation of section 1201." The Copyright Office also noted that "Congress and other agencies may be best positioned to act on this emerging issue." General counsel for the Copyright Office reiterated in a press briefing that the Copyright Office reviews Section 1201 exemptions not through an overall policy lens, but rather through the more narrow lens of what Section 1201 authorizes the Copyright Office to do. The office has thus deferred to Congress and various policymakers on the broader issue of permitting access to AI systems for research or other reasons. In the meantime, researchers or other parties seeking access to AI systems must be wary of Section 1201's prohibition on circumvention, as well as a host of other potential restrictions to unauthorized access, such as contractual provisions, a growing body of law concerning web scraping, and statutory provisions such as the Computer Fraud and Abuse Act.

# FTC Settles Case Against Company for False and Misleading Claims About Its AI Facial Recognition Technology

On January 13, 2025, the FTC finalized a consent order to settle allegations that IntelliVision Technologies Corp. (IntelliVision) made false, misleading, or unsubstantiated claims that its AI-powered facial recognition software was free of gender and racial bias. IntelliVision's facial recognition software is incorporated into various consumer products, including smart home security systems. According to the FTC's complaint, IntelliVision did not have any support for its claim that its software had "one of the highest accuracy rates on the market and performs with zero gender or racial bias." Additionally, IntelliVision allegedly claimed that it trained its AI-powered software on millions of images when it trained the software on the facial images of only around 100,000 unique individuals, then created variations of those same images to fill out the rest of its training data set.

Among other things, the order prohibits the defendants from misrepresenting the capabilities of its facial recognition software's accuracy and efficacy, the comparative performance of its facial recognition technology with respect to categories of individuals, or the accuracy or efficacy of its facial recognition technology at detecting spoofing.

# New York Department of Financial Services Provides Cybersecurity Guidance on AI

On October 16, 2024, the New York Department of Financial Services (NY DFS) issued an Industry Letter (the Letter) addressing cybersecurity risks stemming from AI and strategies to mitigate them. The Letter is addressed to entities regulated by NY DFS and does not impose new requirements; instead, it provides companies with guidance to meet existing obligations under 23 NYCRR Part 500, a cybersecurity regulation adopted in 2017.

NY DFS's guidance highlights four key risk categories associated with AI:

1. AI-Enabled Social Engineering

   Companies face the persistent threat of social engineering, and AI has enhanced the ability of threat actors to create more personalized and sophisticated content. Threat actors are increasingly relying on AI to craft deepfake content and execute phishing schemes, aiming to manipulate authorized users into divulging nonpublic information about themselves and their employers. Some such content may convince users to take actions that they otherwise would not commit (e.g., share credentials or take unauthorized actions such as wiring funds to fraudulent accounts), while other content may be used to impersonate the user's appearance or voice so as to circumvent biometric verification technology or otherwise authenticate that individual.

2. AI-Enhanced Cybersecurity Attacks

   Threat actors have adopted AI to scale up cybersecurity attacks in new and concerning ways. Due to its ability to rapidly ingest and assess information about information systems, AI can allow threat actors to quickly and efficiently identify and exploit security vulnerabilities; once inside an organization's information systems, AI can be used to conduct reconnaissance to determine, for example, how best to deploy malware and access and exfiltrate nonpublic information (NPI). Furthermore, threat actors can leverage AI to avoid detection and bypass defensive security controls. The increased proliferation of publicly available AI-enabled products and services also lowers the barriers to entry for threat actors by decreasing the amount of cybersecurity knowledge needed to run a successful cyberattack.

3. Exposure of Vast Amounts of Nonpublic Information

   Products that use AI typically require the collection and processing of substantial amounts of data, often including NPI. Companies that develop or deploy AI products may need to maintain NPI in large quantities. This poses additional risks because this vast quantity of data

*Continued on page 16...*

## New York Department of Financial Services Provides Cybersecurity . . . *(Continued from page 15)*

makes them prime targets for threat actors. For example, companies that collect biometric data could be targeted by threat actors who wish to use this information to impersonate authorized users to gain access to NPI, generate AI-enabled social engineering, and bypass multifactor authentication (MFA).

4. Increased Vulnerabilities Due to Third-Party, Vendor, or Other Supply Chain Dependencies

   Companies that work with third-party vendors to provide data for their AI products may expose themselves to additional vulnerabilities. Third-party vendors, if compromised by a cybersecurity incident, could expose a company's NPI and become a gateway for broader attacks on that entity's network, as well as all other entities in the supply chain.

*Key Mitigation Strategies*

The NY DFS Letter outlines several mitigation strategies that entities can adopt to mitigate cybersecurity threats relevant to their businesses, including those posed by AI:

1. Comprehensive Risk Assessments

   Companies subject to 23 NYCRR Part 500 must maintain cybersecurity programs, policies, and procedures that are based on cybersecurity risk assessments. These assessments should identify the AI technologies currently in use, their purpose, and how cybersecurity threats may result in the misuse of AI, and they must be updated at least annually. In addition, covered entities must establish, maintain, and test plans that contain proactive measures to investigate and mitigate cybersecurity events and other disruptions, including those relating to AI.

2. Due Diligence on Third-Party Service Providers

   When conducting due diligence on third-party service providers before allowing access to information systems and NPI, covered entities should evaluate the cybersecurity risks posed by AI products and services, among other factors. The Letter highlights the importance of contractual obligations requiring vendors to implement strong countermeasures for cybersecurity attacks and promptly notify entities in the event of an AI-related incident. Providers should also align with the company's overall cybersecurity strategy to ensure seamless risk management.

3. Implementing Robust Access Controls

   The NY DFS flags in the Letter that multi-factor authentication (MFA) is one of the most effective access control measures and notes that it will be a requirement in certain circumstances starting late next year. The Letter encourages covered entities to implement advanced access controls, such as using more than one biometric modality to confirm a user's identity. In addition to MFA, 23 NYCRR Part 500 requires covered entities to have other access controls in place that limit the NPI a threat actor can access in case MFA fails to prevent a threat actor from gaining unauthorized access to information systems.

4. Monitoring and Data Management

   The Letter advises companies permitting employee usage of AI applications to implement training programs focused on monitoring and identifying new security vulnerabilities, such as unusual search behaviors or the exposure of NPI to public AI-enabled products. Additionally, companies should adopt robust data management practices to safeguard their information systems. These practices may include data minimization, establishing appropriate controls, and maintaining an up-to-date inventory of systems utilizing AI.

# Data Center Infrastructure and National Energy Policy Dramatically Collide at FERC

Prior to 2024, the Federal Energy Regulatory Commission (FERC), which oversees the interstate sale and transmission of electricity, had essentially no policy or precedent specifically addressing the provision of power to data centers. That is about to change, with potentially significant implications for whether, how, and on what timeline data centers can be built and powered, amidst historically high, AI-fueled demand growth. Due to a flurry of filings by certain utilities, independent power producers, and PJM Interconnection, L.L.C. (PJM), i.e., the transmission system operator and market administrator for the nation's largest power market, FERC currently has several high-profile, contentious proceedings underway which raise numerous difficult policy questions. As a result, FERC now finds itself at the center of a national debate over how to satisfy the nation's demand for the data infrastructure needed for AI compute.

The flurry of activity began with PJM's filing to modify the Susquehanna nuclear facility's generator interconnection agreement to accommodate a behind-the-meter data center that the facility's owner agreed to sell to Amazon. That filing garnered significant participation from a wide range of stakeholders with interest in such "co-location" arrangements and their policy implications. Certain utilities engaged in the proceeding to call into question the lawfulness of arrangements, which in turn produced intense backlash from various other entities that see such arrangements as not only lawful but also the only viable option for satisfying the nation's computing needs in the near- to medium-term given that it takes many years and much higher cost to build the transmission system facilities needed to serve data centers that do not rely on an existing interconnection to the transmission system. On November 1, 2024, FERC rejected PJM's filing in a 2-1 vote, with the agency's then-Chairman issuing a forceful dissent and two of the agency's five Commissioners recusing themselves from the proceeding for unstated reasons. The two Commissioners who voted to reject the filing adopted an ambiguous rationale that many view as having troubling policy implications, signaling that those two Commissioners are perhaps disinclined to support the rapid interconnection of data center infrastructure. In his dissent, the then-Chairman emphasized that rejecting the filing represents a risk to the nation's security, economic competitiveness, and grid reliability. Certain independent power producers have requested that the agency change course in the proceeding by granting rehearing or clarification of its decision. FERC has not yet acted on those requests.

That proceeding on the co-located Susquehanna/Amazon facility has spawned multiple other proceedings, each of which raises various broader policy issues beyond the context of the co-located Susquehanna/Amazon facilities. The follow-on proceedings include, among other things, utility filings that seek to force data centers to pay for transmission system costs even if the load is served exclusively by a co-located generator, a petition from certain utilities asking FERC to declare that co-location arrangements cannot be facilitated through FERC-jurisdictional generator interconnection agreements, a complaint filed by an independent power producer which seeks to reform PJM's interconnection and market rules to accommodate data center co-location arrangements, and a generic administrative proceeding that FERC initiated of its own accord to explore various policy issues related to data center load growth and the use of co-location arrangements to meet it. Unrelated to those proceedings, the FERC recently approved what appears to be the first application for approval under section 203 of the Federal Power Act for a data asset technology company's acquisition of a renewable generation facility to power its digital assets. More section 203 proceedings like that one seem inevitable. What actions FERC will take, and what policies it will enact, in these various proceedings remains to be seen. However, some things are clear:

- these contests are only the first wave of issues caused by AI-driven demand growth in the U.S., given our aging grid infrastructure and associated delays in construction of new generation;
- resolution will create winners and losers, and could cause a fraught reshuffling of burdens and benefits among categories of energy consumers; and
- the federal regulatory landscape for powering data center infrastructure is poised for change, likely significant change, in 2025.

# Deal Highlights

**Wilson Sonsini Advises Anthropic in Connection with Expanded Collaboration with Amazon**

On November 22, 2024, Anthropic announced an expansion of their previously announced collaboration with Amazon Web Services (AWS), deepening their partnership to develop and deploy advanced AI systems. This expanded partnership includes a new $4 billion investment from Amazon and establishes AWS as their primary cloud and training partner. This will bring Amazon's total investment in Anthropic to $8 billion, while maintaining their position as a minority investor. Wilson Sonsini Goodrich & Rosati represented Anthropic in the commercial aspects of the transaction.

Together with AWS, Anthropic is laying the technological foundation—from silicon to software—that will power the next generation of AI research and development. By combining Anthropic's expertise in frontier AI systems with AWS's world-class infrastructure, the partnership is building a secure, enterprise-ready platform that gives organizations of all sizes access to the forefront of AI technology.

**Wilson Sonsini Advises Socure on $136 Million Acquisition of Effectiv**

On October 24, 2024, Socure, the leading provider of AI for digital identity verification, fraud prevention, and sanction screening, announced that it has signed an agreement to acquire Effectiv, a real-time risk decisioning company, for $136 million. Wilson Sonsini Goodrich & Rosati advised Socure on the transaction.

The strategic acquisition pairs Socure's best-in-class digital identity verification and fraud solutions with a developer-friendly AI orchestration and decisions platform. With this acquisition, Socure—which serves more than 2,700 customers and has verified more than 2.26 billion identities over the past 12 months—further solidifies its leadership position in the identity verification and fraud prevention market, and is propelled into the $200 billion enterprise fraud industry, which additionally encompasses payments fraud, credit underwriting, and AML transaction monitoring.

**Wilson Sonsini Advises Insider on $500 Million Series E Financing**

On November 1, 2024, Insider, a leading AI-native omnichannel experience and customer engagement platform, announced a $500 million Series E funding round led by General Atlantic, a leading global growth investor. Wilson Sonsini Goodrich & Rosati advised Insider on the transaction.

Insider plans to further develop its next-generation marketing software offering and invest heavily in research and development, focusing on expanding and evolving its AI solutions. The company also intends to scale its talent base and geographic footprint, leveraging General Atlantic's global platform. With an established market position in 28 countries across five continents, including North America, EMEA, APAC, and Latin America, Insider plans to increase its regional investments on the back of strong demand in the U.S. market, where it has achieved significant growth. Additionally, the company will use the funds to explore strategic M&A opportunities.

**Wilson Sonsini Advises Stepful on $31.5 Million Series B Round**

On November 13, 2024, Stepful, a company re-imagining healthcare training for allied health professional jobs, announced it successfully raised $31.5 million in Series B funding. The round was led by Oak HC/FT with participation from Y Combinator, Reach Capital, AlleyCorp, Company Ventures, Green Sands, ECMC Education Impact Fund, Intermountain Ventures, and others. Wilson Sonsini Goodrich & Rosati represented Stepful in the transaction.

Stepful offers educational training programs for both entry-level positions,

*Continued on page 19...*

## Deal Highlights . . . *(Continued from page 18)*

including medical assistants, medical admins and pharmacy technicians, and advanced programs for licensed practical nurses and surgical technicians. Unlike other trade schools, Stepful is an AI-powered learning platform with an accelerated format, lower costs and placement for students who successfully complete the program. To date, the company has seen strong growth in its business, expanding from 50 students in 2021 to more than 30,000 enrollees projected in 2024. With this new funding, Stepful will expand its B2B offering and continue growing its health system partnerships.

**Wilson Sonsini Advises Tenstorrent on $693 Million Series D Financing**

On December 2, 2024, Tenstorrent, a next-generation computing company that builds computers for AI, announced the closing of over $693 million in its Series D funding round, at a pre-money valuation of $2 billion. Samsung Securities and AFW Partners led the round, with participation from XTX Markets, Corner Capital, MESH, Export Development Canada, Healthcare of Ontario Pension Plan, LG Electronics, Hyundai Motor Group, Fidelity Management & Research Company, Baillie Gifford, Bezos Expeditions, and more. Wilson Sonsini Goodrich & Rosati advised Tenstorrent on the transaction.

Tenstorrent plans to use the funding to build out open-source AI software stacks, hire developers, expand its global development and design centers, and build systems and clouds for AI developers.

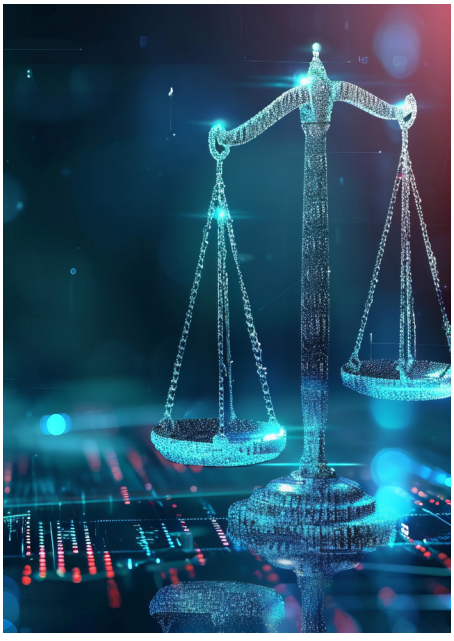
**Wilson Sonsini Advises EzDubs on $4.2 Million Seed Round**

On December 11, 2024, EzDubs, a speech translation start-up using AI, announced that it has raised a $4.2 million Seed round and launched its flagship solution out of beta: the first and only app that translates calls into other languages as you're speaking, preserving your voice and emotions. "Much like Star Trek's Universal Translator," EzDubs enables people who don't speak each other's languages to communicate by voice live and remotely. The previously unannounced funding round was led by Rahul Garg and Neeraj Arora during their tenure at Venture Highway. Other participants in the round were Y Combinator and well-known angel investors.

# Wilson Sonsini AI Advisory Practice Highlights

Wilson Sonsini attorneys provided AI-related guidance at the following events:

- On November 20 and November 21, respectively, Yann Padova and Laura De Boel discussed AI regulation and the interaction between the AI Act and the GDPR at the IAPP Europe Data Protection Congress.
- On November 12, Matthew Nuding discussed how the Information Commissioner's Office is approaching AI regulation at the Society for Computers and Law.
- On November 10, Gary Greenstein spoke at the Generative Series' AI and Music Program about differences in perception and experience between manmade and AI generated music.
- On October 30, Jordan Jaffe discussed evolving rules, guidance, and court decisions regarding the patentability and copyrightability of inventions involving GenAI outputs, who owns those rights, and how to protect the business while remaining competitive at an Ad Idem Network event.
- On September 26, Andrea Linna spoke at the ABA Healthcare Delivery & Innovation Conference about privacy concerns, regulatory compliance, liability issues, and the ethics of AI decision-making in healthcare.



# Newsletter Contributors

- Laura Ahmed
- Julia Anderson
- Matthew Bogdan
- Evan Burroughs
- Deirdre Carroll
- Jess Cheng
- Laura De Boel
- Lizzy Doctorov
- Logan Fahrenkopf
- Sophia Galleher
- Julius Giesen
- Nic Gladd
- Todd Glass
- Joshua Gruenspecht
- Katie Gu
- Tarek Helou
- Eddie Holman
- Yeji Kim
- Jindrich Kloub
- Angelica Lee
- Maneesha Mithal
- Peter Mostow
- Chris Murray
- Stacy Okoro
- Bryan Poellot
- Manja Sachet
- Alyza Sebenius
- Taylor Stenberg Erb
- Hayden Stephens
- Hattie Watson
- Malcolm Yeary
- Vicky Zhou
- Scott Zimmermann

The following attorneys have editorial oversight of Wilson Sonsini's All Eyes on AI: Regulatory, Litigation, and Transactional Developments.

**Laura De Boel**
ldeboel@wsgr.com

**Jordan R. Jaffe**
jjaffe@wsgr.com

**Scott McKinney**
scmc@wsgr.com

**Maneesha Mithal**
mmithal@wsgr.com

**Manja Sachet**
msachet@wsgr.com

WILSON SONSINI

650 Page Mill Road, Palo Alto, California 94304-1050 | Phone 650-493-9300 | Fax 650-493-6811 | www.wsgr.com

Wilson Sonsini has 19 offices in technology and business hubs worldwide. For more information, visit wsgr.com/offices.