

开放权重与美国 AI 领导力

2026 年 7 月 24 日

20 世纪 80 年代,早期的开源软件先驱质疑了当时盛行的观点——即只有在企业对代码保持严格控制的情况下,软件才能向前发展。这场运动推动建立了一个透明的生态系统,让全球开发者都能学习、修改和改进软件。如今,由开源社区开发的软件支撑着互联网的绝大部分,并成为全球顶尖科技公司、美国军方以及开展科学研究、网络安全和其他关键任务的联邦机构所使用系统的基础。开源不仅降低了软件成本,更开创了一个共享知识的基础,一代又一代的美国工程师和创业者在此基础上建立了自身的制度主权。

如今,美国在 AI 领域面临着类似的抉择。衡量我们 AI 领导力的标准,不在于单一的前沿 AI 模型,而在于美国能否构建一个能够渗透扩散至各个行业的强大、开放的生态系统。这对于在全国范围内创造创新与繁荣的机遇至关重要。这需要扩大获取 AI 的机会、鼓励竞争、培育强健的应用层,并赋予美国人对其所依赖之技术更大的控制权。开放权重模型(即任何人都可以下载、审查、修改并在自己的基础设施上运行的 AI 模型)是这一基础的重要组成部分,因为它们使先进的 AI 更加触手可及、易于适配且广泛可用。

开放权重扩大了进入 AI 经济的途径。初创企业、成熟公司、大学和公共机构可以在先进模型的基础上进行开发,而无需从零开始训练模型,也不必为每一项任务都支付前沿级别的模型使用费。开放权重让每个机构都能以恰当的成本将合适的模型应用于合适的工作,将前沿规模的能力留给真正的前沿难题,而在其他所有地方运行高效的专用模型。随着 AI 应用规模扩展到每天数十亿次日常任务,这种严谨高效的资源匹配正是让 AI 在经济上具备可持续性的关键所在。美国赢得 AI 时代的方式,就是将 AI 渗透扩散到工厂、医院、农场、教室以及千家万户企业的日常工作流程中。

开放权重还能增强竞争,而竞争能确保 AI 带来的红利被广泛共享,而不是集中在少数人手中。通过允许众多机构构建、适配和部署先进模型,开放权重不仅在模型开发者之间形成了竞争,也推动了云芯片、应用和服务等全方位的良性竞争。这种竞争能够激发创新、降低成本,并使 AI 的收益广泛惠及整个经济体。

开放权重还给予客户更大的控制权。随着各机构在 AI 领域进行投资,他们希望确信自己不会被锁定在单一供应商身上,也不会失去随时间推移积累起来的知识和能力。开放权重模型有助于提供这种保证,它允许机构控制自己的数据,根据自身需求评估和适配模型,并根据业务需求灵活部署。随着各机构利用 AI 创造价值,开放权重使其能够通过自适应改进的模型、专业化能力以及不断积累的知识来拥有这些价值,从而推动美国的自主权与繁荣。

诚然,开放权重确实存在明确且真实的风险。权重一旦发布,就会超出原开发者的控制,修改后的版本也很难追踪或逆转。但应对这种风险的正确做法并非禁止开放权重。在一个网络安全攻击者使用先进 AI 的世界里,防御者同样需要获取具备相当能力的模型,以便检测、模拟并响应新出现的威胁。开放模型拓展了防御能力,提高了透明度,并使安全漏洞能够在多个团队的协同下被发现和修复。

事实上,开放可能是实现 AI 安全与可靠最关键的途径之一。仅仅依赖封闭模型本质上并不安全:它们可能被破解、滥用,或以外界无法察觉的方式发生故障。而将先进的 AI 能力集中在少数几个封闭模型之后,会加剧这种风险。这会导致出现少数几个单点故障风险,削弱竞争,并将关键技术留给少数几家供应商控制。相反,开放权重模型允许广大研究人员和开发者社区审查模型行为、识别漏洞、制定安全保障措施,并在实践中不断改进它们。正如开源软件证明了透明度可以比隐蔽性更安全一样,AI 安全可能取决于让更多人有能力测试和强化社会所依赖的模型。它能够实现严谨的基准测试与评估、红队演练,以及针对真实且已被证实的危害采取针对性保护措施,而不是默认假定封闭系统更安全。

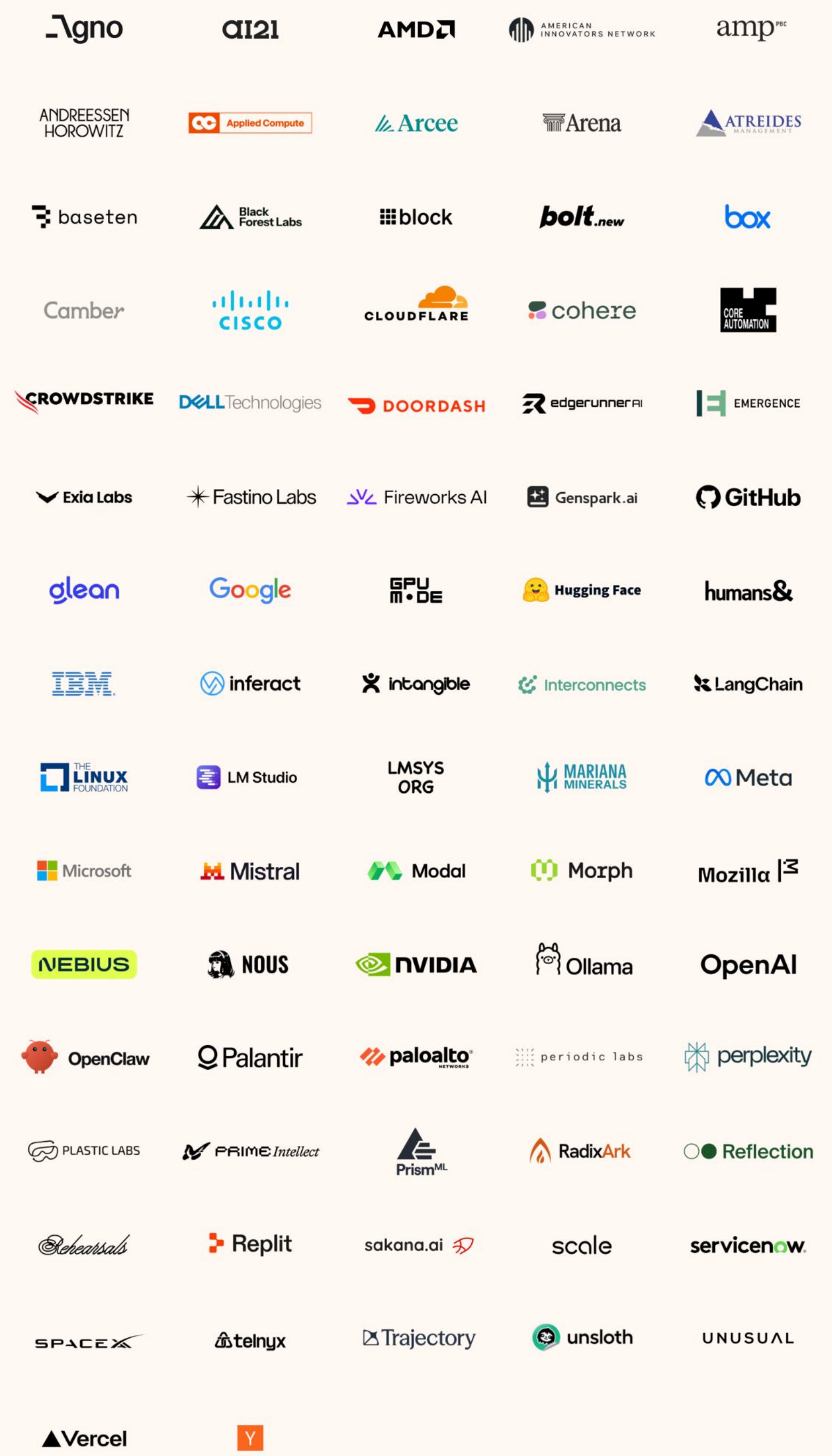
构建强大的 AI 生态系统并非理所当然。政策制定者面临着采取行动的关键契机。这包括:为初创企业和研究人员扩大算力获取渠道,投资于共享训练资源(数据集、工具、评估框架),以及避免对开放模型实施过早的限制(以免扼杀竞争或将创新推向海外),从而保持前沿领域的多元化。这些举措还必须关注如何通过强健的应用层,在整个经济体内扩大 AI 的自主化应用。

在塑造这一生态系统时,政策制定者应谨慎避免将合法的模型开发技术与非法侵占混为一谈。“蒸馏”(即利用一个模型的输出来帮助训练或改进另一个模型的做法)是一种广泛用于模型改进、评估和验证的技术。它体现了学习、继承和改进现有技术的悠久传统,而正是这一传统自开源软件运动兴起以来推动了创新的飞跃。相比之下,试图从封闭模型中非法榨取价值的行为确实引发了合理的担忧。对于这些担忧,应当通过有针对性的法律和商业框架来解决,而不是对在 AI 创新中发挥重要作用的技术采取“一刀切”的限制措施。

AI 时代可以是一个走向繁荣的时代。做出正确的选择,开放权重 AI 就能扩大机遇、增强竞争、延续美国的技术领导地位、降低风险,并确保这一非凡技术带来的收益广泛惠及整个经济体。这样一个未来值得去打造,而美国应当在其中发挥引领作用。

联合签署方

Agno • AI21 • 超微半导体 (AMD) • 美国创新者网络 (American Innovators Network) • AMP • Andreessen Horowitz • Applied Compute • Arcee AI • Arena • Atreides Management • Baseten • Black Forest Labs • Block • Bolt • Box • Camber • 思科 (Cisco) • Cloudflare • Cohere • Core Automation • CrowdStrike • 戴尔科技 (Dell Technologies) • DoorDash • EdgeRunner • Emergence Capital • Exia Labs • Fastino Labs • Fireworks AI • Genspark • GitHub • Glean • 谷歌 (Google) • GPU MODE • Hugging Face • humans& • IBM • Inferact • Intangible • Interconnects AI • LangChain • Linux 基金会 (The Linux Foundation) • LM Studio • LMSYS • Mariana Minerals • Meta • 微软 (Microsoft) • Mistral • Modal • Morph • 谋智基金会 (Mozilla) • Nebius • Nous Research • 英伟达 (NVIDIA) • Ollama • OpenAI • OpenClaw • Palantir • Palo Alto Networks • Periodic Labs • Perplexity • Plastic Labs • Prime Intellect • Prism^{ML} • RadixArk • Reflection • Rehearsals • Replit • Sakana AI • Scale • ServiceNow • SpaceX • Telnix • Trajectory • Unsloth • Unusual Ventures • Vercel • Y Combinator



所有商标和商标名称均为其各自所有者的财产。