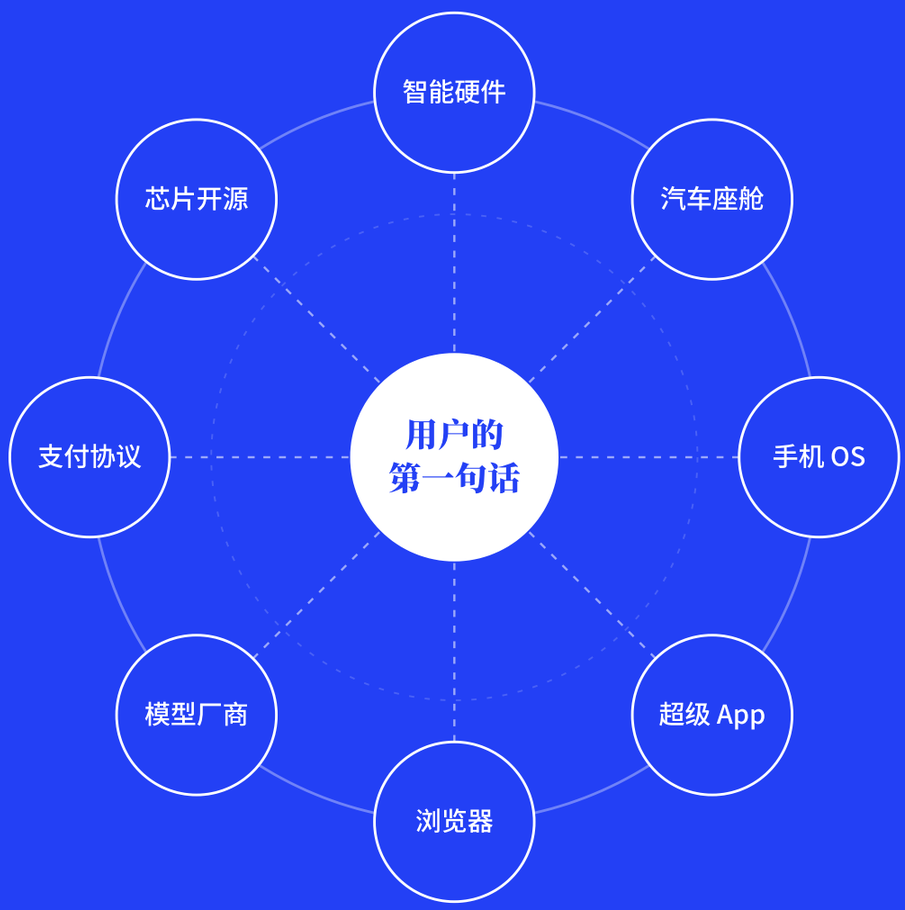
PERSONAL AGENT · 个人智能体产业研究

代理人时代

入口、信任与权益的重新分配



竞争的主战场，已经从模型能力，转向入口、信任和权益分配。

个人智能体产业研究报告 2026
2026-10-30 · Joyceshang

目录

数据截至 2026 年 10 月
13 张图表 · 10 条预测

00 **执行摘要** 03
七个核心结论与终局判断

01 **研究范围、定义与方法** 04
懂你、替你做、一直在、代表你

02 **市场拐点** 05
2026 年，个人智能体进入规模化竞争

03 **技术** 07
架构正在收敛，信任是最大短板

04 **竞争格局** 09
资源禀赋决定路线，中美走向两种格局

05 **用户体验** 11
从“操作工具”到“委托一个人”

06 **商业模式与商家生态** 12
谁付钱，agent 就为谁服务

07 **权益边界与监管** 14
用户的议价力将被重写

08 **未来情景与关键预测** 16
前台归一、后台垂直；十条可验证预测

09 **对各类参与者的战略建议** 18
八类角色的核心问题与行动

A–C **附录** 19
待核实事项、术语、主要来源

终局判断

前台归一、后台垂直；一个记忆，多个设备入口；最终形成“用户侧 agent”与“平台侧 agent”的对峙。

EXECUTIVE SUMMARY

竞争的主战场，已从模型能力转向入口、信任和权益分配

2026 年是个人智能体从概念走向规模化竞争的一年。七个结论，概括这场竞争的走向。

01 市场已过拐点

2026 年 9 月 Meta Muse 上线后一个月内，OpenAI、Manus、阿里、字节、腾讯、蚂蚁相继推出或曝出个人智能体；Google 早在 5 月已发布 Gemini Spark。八类玩家在争抢同一个位置：用户“第一句话”交给谁。

02 架构正在收敛

主流做法是给每个 agent 配一台云端专属电脑，并逐步向本地设备延伸；安全设计从“让模型守规矩”转向“在模型外立边界”。

03 能干活，还不能托付

模型、工具连接、云端运行环境已经成熟；长任务可靠性、提示注入防御、agent 身份与授权、记忆迁移、常驻成本仍是短板。下一阶段瓶颈是信任基础设施。

04 资源禀赋决定路线，中美分化

美国由模型公司与操作系统主导独立 agent；中国呈现系统级 agent 与超级 App 对峙，模型厂商借生态或合作穿插。

05 体验的本质是委托

衡量标准从使用时长转向“用户敢交出多少”；渐进授权与可接管会成为标配。

06 谁付钱，agent 就为谁服务

常驻 agent 每个用户都有固定算力成本，订阅将是主流；广告与“代表用户”天然冲突；商家一侧的流量分配权从“排序”转向“agent 的判断”。

07 权益边界将被重写

记忆将走向“有限可携带”，路径类似携号转网；忠诚义务将从金融、健康等高风险场景开始落地。

终局判断

前台归一、后台垂直；一个记忆，多个设备入口；最终形成“用户侧 agent”与“平台侧 agent”的对峙。

第八章列出十条可验证预测，第九章给出各类参与者的建议。

01 研究范围、定义与方法

SCOPE · DEFINITION · METHOD

本报告所称“个人智能体”须同时满足四个条件。只满足一到三条的产品，属于过渡形态。

EXHIBIT 00 **四个条件，缺一不可**

01	02	03	04
懂你	**替你做**	**一直在**	**代表你**
有长期记忆，能使用个人数据	能调用工具、操作应用、完成任务	后台常驻、主动提醒、跨设备	获授权后能以用户身份付款、发消息
反例：每次从零开始的聊天机器人	反例：只给建议的问答助手	反例：只有打开才工作的工具	反例：只能看、不能动的助手

研究范围

地域 以中国和美国为主，兼及欧盟监管。

对象 模型厂商、手机操作系统与终端、超级 App、浏览器与 PC、智能硬件、汽车、支付与电商基础设施、芯片与开源社区。

不含 企业内部办公 agent、编程 agent（仅在与个人场景交叉时提及）；垂直健康场景另行研究。

时间 数据截至 2026 年 10 月。

研究方法

资料 厂商发布会与官方文档、主流科技与财经媒体、政府与监管文件、学术与标准提案。

框架 产业链分层、架构原型对比、技术成熟度分档、路线分叉、历史类比、情景推演。

局限 部分数据仅有单一或二手来源，已在附录标注；缺少用户侧的留存和使用数据。

读者须知 全文以蓝底色块标出的“本报告判断”为分析结论，而非事实；事实部分均有公开来源，见各页页脚与附录。

THE TIPPING POINT

02 2026，个人智能体进入规模化竞争

2026 年下半年，个人智能体从开源极客圈进入大众市场。触发点是 Meta Muse；之后一个月内，中美大厂密集跟进。

EXHIBIT 01 **2026 年关键事件**

01-15	**阿里**	千问接入淘宝、支付宝，上线 400 多项办事功能
02-14	**OpenClaw**	作者加入 OpenAI，项目转交基金会
05-19	**Google**	发布 7×24 个人 agent Gemini Spark
09-07	**华为**	HarmonyOS 7 升级为 Agent 亲和架构
09-08	**Meta**	**Muse 在美国上线 · 拐点**
09-14	**苹果 / 字节**	iOS 27 推出 Siri AI；豆包手机助手消费者版发布
09-22	**阿里**	宣布加速打造 Personal Agent，发布 AI 眼镜与耳机
09-28	**Manus**	发布个人 agent 应用 Cue
09-29	**OpenAI**	发布常驻式 agent Dots
09-30	**腾讯**	元宝将推个人智能体（媒体报道）
10-09	**字节**	个人助理项目 Spell 加速，与豆包结合
10-13	**阿里**	Personal Agent「千问 Go!」开放体验申请

META MUSE · 上线 12 天

280 万

次下载（约）

8 类玩家

在争抢同一个位置：用户“第一句话”交给谁。

1 个月

Muse 上线后，OpenAI、Manus、阿里、字节、腾讯相继推出或曝出个人智能体。

三个信号：这是拐点，而非热点

产品形态收敛

常驻云端、连接账号、长时自主、关键节点确认，成为各家共同骨架。

开源先行、大厂跟进

OpenClaw 2026 年初爆红后，Google、Meta 的产品都被视为对它的回应。

付费档位出现

Muse 设 20/100 美元档，OpenAI 新增 500 美元档，豆包推出 68/200/500 元专业版。

来源：界面新闻（Muse 下载量） · ProPakistani（Dots） · The Next Web（Spark）

EXHIBIT 02 个人智能体产业链全景 · 8 层

八类玩家，争夺同一个位置：用户的第一句话

用户的一句话，交给谁来办?

入口

L1	智能硬件	Meta 眼镜 · 千问眼镜与耳机 · OpenAI 设备 · Google 眼镜
L2	汽车座舱	鸿蒙座舱小艺 · 理想 × 高德 · 蔚来 · 高通车端 Claw
L3	手机 OS	苹果 Siri · Gemini Intelligence · 小艺 · YOYO · 小爱 · 小布
L4	超级 App	微信 · 支付宝 · WhatsApp · 亚马逊 Alexa
L5	浏览器与 PC	Chrome · Comet · Edge Copilot · Windows
L6	模型与原生应用	OpenAI Dots · Gemini Spark · Meta Muse · Claude · Manus Cue · 豆包 · 千问 Go! · 元宝
L7	支付与协议	UCP · AP2 · ACP · MCP · A2A · 支付宝 AI 付
L8	芯片与开源	高通 · 苹果 · 华为 · OpenClaw · 开放权重模型

底座

八类玩家用各自最强的牌争抢同一个位置。越靠近用户的层，越接近入口；底层的协议、支付与芯片，则决定各方能否互通。

TECHNOLOGY

03 架构正在收敛，信任是最大短板

四种架构原型并存，但“给每个 agent 配一台云端专属电脑”已成主流，并正在向本地设备延伸。

EXHIBIT 03 **四种架构原型**

原型 A

本地自托管

住在哪
用户自己的电脑或服务器

代表
OpenClaw

＋ 优势
数据在本地、模型自选

－ 劣势
安全靠用户自己，门槛高

原型 B · 主流

云端专属电脑

住在哪
厂商为每个 agent 分配的云端虚拟机

代表
Gemini Spark、OpenAI Dots、Meta Muse、Manus Cue

＋ 优势
设备关机也能工作，审批边界在平台侧

－ 劣势
每用户固定算力成本

原型 C

生态内嵌

住在哪
自家超级 App 内

代表
千问 Go!、支付宝阿宝

＋ 优势
办事闭环最短

－ 劣势
能力限于自家生态和入驻伙伴

原型 D

系统端侧

住在哪
手机操作系统内

代表
豆包手机助手、小艺、Siri

＋ 优势
能读本地数据、看屏幕

－ 劣势
跨品牌不互通，调用第三方受限

两个值得关注的趋势

云 ⇄ 端

云与端在会合

云端产品开始伸手到用户本机：Dots 可选连接用户的电脑，Spark 的 macOS 版可读本地文件。纯云端与纯本地的界线正在模糊。

模型之外

安全边界移到模型外

Muse 把凭证放在运行容器之外，用独立的 Sentinel 守门，审批可按单次到永久分级授权。反面是 OpenClaw：2026 年暴露多个安全漏洞，并被 CNCERT 发布安全提示。

一句话

安全设计正在从“让模型守规矩”，转向“在模型外立边界”。

来源：MindStudio · TechCabal · The Batch · ThaiCERT

能干活，还不能托付。

最具说服力的证据来自电脑操作评测：单步能力已经过关，串成长任务仍不可靠。

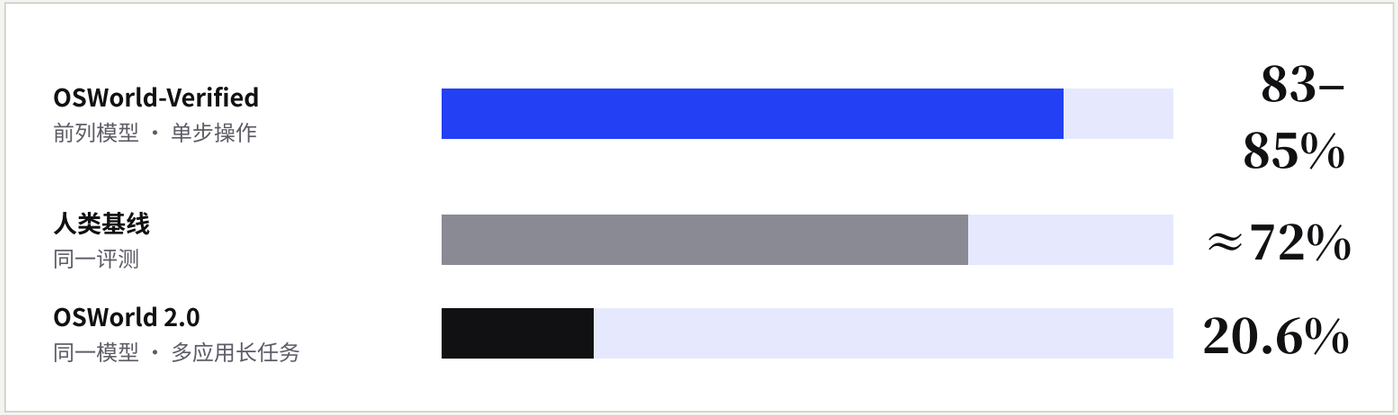


EXHIBIT 04 **技术模块成熟度 · 4 档（本报告判断）**

成熟	可用但不稳	早期	未解决或空白
模型理解与推理	电脑与浏览器操作	主动与打扰管理	提示注入防御
工具连接（MCP、插件）	手机 GUI 操作	支付授权	agent 身份与授权标准
云端沙箱运行时	记忆存取	agent 间协作	记忆跨平台迁移
	端侧模型	评测与审计	常驻成本

提示注入：OpenClaw 承认是全行业未解决的问题；Muse 的设计前提就是“注入迟早会发生”。

记忆迁移：三大助手的导入导出只是一次性快照。

身份与授权：尚无互通标准证明“哪个人授权哪个 agent 做了什么”，IETF 已有草案。

常驻成本：即使用户不用，常驻 agent 也占着一台云端虚拟机。

本报告判断

下一阶段的竞争不在模型参数，而在谁先补齐信任基础设施。agent 身份与授权的事实标准，更可能由支付网络和大平台推动（如 Visa、万事达与 Cloudflare 的 agent 验证），而不是标准组织。

来源：Crypto Briefing · youngju.dev · IETF 草案

04 资源禀赋决定路线

COMPETITIVE LANDSCAPE

做一个个人智能体，要在八个关键问题上做选择。每家的答案，都押在自己最强的那张牌上。

EXHIBIT 05 **关键技术路线分叉与各家选择**

1	**agent 住在哪** 本地 / 云端虚拟机 / 自家 App / 手机系统	**本地** OpenClaw **云端** Spark、Dots、Muse、Cue **App** 千问 Go!、阿宝 **系统** 豆包手机助手、小艺、Siri
2	**产品形态** 独立 App / 内嵌 / 系统级 / 自有硬件	**独立** Muse、Cue **内嵌** Dots、Spark、千问 Go! **系统级** 苹果、华为、Google **硬件** OpenAI、千问、Meta
3	**大脑从哪来** 自研 / 借用 / 用户自选	**自研** OpenAI、Google、Meta、阿里、字节、华为 **借用** 苹果借 Gemini **自选** OpenClaw
4	**怎么动手** 协议优先 / GUI 优先	**协议** 小艺、千问、Spark、Dots **GUI 兜底** 豆包
5	**记忆放哪** 用户可见的文件 / 平台托管 / 端侧本地	**文件** OpenClaw **托管** Dots、Muse、Spark **本地** 豆包、小艺
6	**agent 的身份** 代用户行事 / 独立身份	**代用户** Muse、千问、豆包 **独立** Cue（自己的邮箱、电话、钱包）
7	**安全边界放哪** 模型外硬边界 / 平台审批 / 用户自担	**硬边界** Muse、Dots **平台审批** Spark、千问、豆包 **用户自担** OpenClaw
8	**一个还是一群** 单个全能 / 总管 + 专职	**单个** Muse **多个** Cue、Dots、小艺（调度 2,000 多个鸿蒙智能体）

最多人选的

云端常驻 + 协议优先 + 平台托管记忆

最激进的

Cue：给 agent 独立的邮箱、电话和钱包

最开放的

OpenClaw：本地、模型自选、记忆是文件

各家都押在自己最强的牌上

EXHIBIT 06 **玩家战略画像**

玩家	核心资产	战略选择	主要风险
Google	模型、Android、Workspace、Chrome 全栈	云端常驻与系统级并行；主导 A2A、UCP、AP2 协议	反垄断与隐私监管
OpenAI	最大的对话用户池与模型	内嵌 ChatGPT、插件补服务、自建硬件	无系统、无交易生态；站内结账已撤回
Meta	社交关系链、WhatsApp、眼镜	独立 App + WhatsApp；主打生活场景；最重的安全隔离	隐私信任底子薄；被亚马逊封禁
苹果	终端与隐私口碑	系统层 + 端云结合；模型借 Gemini	自研滞后；首发不含欧盟与中国
华为	操作系统与全场景设备	系统接管应用分发，协议优先	超级 App 是否配合
阿里	电商、支付、出行生态	内嵌千问 App，开放平台接第三方；眼镜补感知	生态外服务覆盖
字节	模型与流量（豆包月活超 3.8 亿）	借手机厂商系统层、GUI 兜底、谈判拿接口	被超级 App 封限（一代已发生）
腾讯	微信关系链与小程序	守住入口，有限开放 A2A；元宝探路	微信全量开放成本高、小程序生态冲突
Manus / OpenClaw	产品速度 / 开源社区	最激进的“agent 即独立的人” / 本地开放	资源与安全

美国

模型公司与操作系统直接推独立的个人 agent，叠加开放的电商与支付协议。用户订阅意愿高，商业模式以订阅为主。

中国

四种力量各守一块：阿里靠生态闭环，微信靠守门，华为靠系统分发，字节靠谈判与合作。

缩影：豆包手机一代通过识别界面操控第三方 App，很快被微信、淘宝和金融类 App 限制，之后转向谈判和标准接口。

本报告判断

美国更可能形成“系统总管”与“独立助理 + 自有硬件”并存的格局；中国更可能是“系统总管”与“超级 App 内的 agent”对峙，模型厂商通过生态（阿里）或合作（字节）穿插其中。

来源：蓝鲸（豆包手机“转正”） · 爱范儿 · C114

USER EXPERIENCE

05 从“操作工具”到“委托一个人”

体验的评判标准不再是界面是否好用，而是用户敢不敢把事交出去、交出去后是否省心。

EXHIBIT 07 **一次委托的六个环节**

01 交代

一句模糊的话就能开始，只问关键问题

Spark 专属邮箱、Muse 进 WhatsApp

02 授权

权限细、默认保守，信任逐步给

Spark 连接默认关闭；Muse 分级审批

03 执行

看得见、停得下、能接管

Dots 可打开云端电脑观看并接管

04 确认

只在关键节点打断，避免确认疲劳

花钱、发邮件前必须审批

05 交付

给结果、替用户做了哪些决定、还剩什么

尚无统一做法

06 兜底

可撤销、有预算上限、有赔付

Cue 钱包预算上限；支付宝“被盗即赔”

确认规则：可撤回 × 代价

	代价小	代价大
可撤回	直接做	做完告知
不可撤回	先问再做	只给建议

五种反面模式

- 确认疲劳
- 黑箱执行
- 过度主动
- 过度拟人与诱导依赖
- 假装完成

其中诱导情感依赖，已被国内《人工智能拟人化互动服务管理暂行办法》明确禁止。

新的衡量指标

委托深度（敢交出的任务难度和金额）· 任务完成率 · 接管率与驳回率 · 主动建议采纳率 · 权限随时间的放宽或收紧

本报告判断

产品核心指标将从“使用时长”转向“委托深度”；渐进授权、可观察、可接管，将成为所有个人智能体的标配。

来源：新华网（拟人化互动服务管理暂行办法）

BUSINESS MODELS

06 谁付钱，agent 就为谁服务

常驻 agent 即使用户不用，也占着一台云端虚拟机。每个用户都有固定成本，“免费 + 广告”很难单独算得过账。

EXHIBIT 08 **七种变现方向**

方向	谁付钱	2026 年实例	卡点
分层订阅	用户	Muse 20/100 美元；豆包 68/200/500 元；千问办公会员 19/49/128 元	重度用户成本高；国内付费意愿低
按用量或额度	用户 / 商家	千问视频额度包；淘天 AI 店小蜜按通计费	花费难预估
广告	广告主	ChatGPT 2 月起上广告，后转按点击计费	与“代表用户”冲突
交易佣金	商家	豆包对 AI 带来的酒店订单收 12%；OpenAI 站内结账 4% 后撤回	交易心智未形成
卖接入与能力	商家	千问开放平台；阿里 Accio Work	商家担心成本与分流
硬件捆绑	用户	豆包手机送会员；OpenAI、千问、Meta 自有硬件	硬件门槛
生态间接变现	不直接收费	用 Alexa for Shopping 的美国用户客单价高 40%	只有大生态用得了

两个关键事实

广告与代理冲突

agent 替用户做选择，一旦收商家的钱，推荐的公正性就会被怀疑。豆包公开强调：现阶段商家不能付费影响排序。

交易心智尚未迁移

66.2% 回 OTA 平台核实

15.2% 直接购买

调研对象：用 AI 做旅行规划的人

来源：Daily AI World · Top Growth · Retail Dive · 虎嗅 · 投资界

从争注意力，到争 agent 的判断

560万
Shopify 商家被默认接入 ChatGPT、Copilot、Gemini

100万+
商家在用 Meta Business Agent

12%
豆包对 AI 带来的酒店订单抽佣；OTA 为 15%–20% 另加广告

EXHIBIT 09 **商家面对的四个新问题**

Q1	怎么被 agent 看见	Shopify 把约 560 万商家默认接入主流 AI 助手；GEO（生成式引擎优化）服务兴起。
Q2	怎么被 agent 接入	千问开放平台让顺丰、自如等以智能体入驻；鸿蒙让服务被小艺调用。
Q3	放不放 agent 进来	据报道亚马逊在 Muse 上线 12 天后封禁了它；Cloudflare 9 月起默认在带广告页面拦截用户 agent；Visa、万事达推出可信 agent 验证。
Q4	给 agent 渠道交多少钱	豆包 12%，对比 OTA 15%–20% 另加广告。

商家也在长出自己的 agent：Meta Business Agent 已有超 100 万商家使用；支付宝“碰一下”把百万级商家设备升级为商家 agent。

> **交易，正在变成用户 agent 与商家 agent 之间的对话。**

本报告判断

订阅将是主流变现方式，美国偏订阅、国内偏佣金和生态；“不卖排序”会成为差异化承诺；商家的流量分配权从“排序”转向“agent 的判断”，“可验证的 agent”会成为电商准入门槛。

来源：Godberry · TechCrunch · TechCrunch · 新浪科技

RIGHTS & REGULATION

07 用户的议价力将被重写

用户交给 agent 的东西，比以往任何时候都多。这些交换的边界，由技术、竞争和规则共同决定。

钱	数据	操作权限	意图	记忆

EXHIBIT 10 **历史上的权力再平衡：先锁定，再松绑**

案例 · 原来的锁定	发生了什么	启示
携号转网 中国 2010–2019 · 换运营商要换号码	2019 年 11 月全国实施；试点省份携转率 1.8%	**迁移权的价值在于约束定价，而非迁移人数**
开放银行 欧盟 PSD2，2018 · 账户数据锁在银行	立法强制开放，英国要求统一 API	**立法强制 + 统一标准，缺一不可**
个人数据可携带权 GDPR、个保法 · 数据留在平台	个保法第 45 条设有限可携带权，需符合网信部门规定条件	**是否适用于 AI 记忆，尚未经过检验**
云服务迁移 欧盟《数据法案》· 高额转出费	2027 年 1 月 12 日起全面禁止转换费	**退出成本可以被监管拿掉**

规律

先锁定，再松绑。

每一次新技术带来新的锁定，最终都由“竞争 + 立法 + 统一标准”把一部分权力还给用户。AI 记忆，可能是下一个。

来源：第一财经 · Oxford Law Blog · 第一财经 · Lindahl

当下的五个争议

01	**记忆可携带**	三大助手 2026 年 3 月上线的导入导出只是一次性快照；MacPaw 7 月提出开放标准 Portable Memory；记忆层公司 Zep 则认为“记忆钱包”不现实，主张靠监管。
02	**忠诚义务**	斯坦福 HAI 主张在金融、医疗等高风险场景对 agent 开发者和部署者施加忠诚义务；商业服务商的消费者条款目前普遍不承担这类义务。
03	**意图经济**	剑桥大学研究者警告：用户的动机和计划，可能被采集、操纵和出售。
04	**数据换价格**	Meta 以用户输入输出换取大幅折扣的“贡献者”档已经出现，目前主要面向开发者。
05	**去中心化**	个人数据仓（Solid）、agent 钱包与 x402 支付协议、开源自托管（OpenClaw）都在推进，但尚未进入大众市场。

国内监管要点

2026-07-15	《人工智能拟人化互动服务管理暂行办法》施行：不得诱导情感依赖、不得情感操纵诱导不合理决策；上线相关功能需做安全评估。
2026-04-30	中央网信办“清朗・整治 AI 应用乱象”专项行动，点名大模型未备案、未标识、利用 GEO 进行“AI 数据投毒”等问题。
待定	个保法第 45 条的可携带权配套条件，将决定 AI 记忆迁移在国内的走向。

本报告判断

记忆将走向“有限可携带”，路径像携号转网：先是厂商为抢用户做导入，再由监管推动统一格式。“数据换价格”将变成明码菜单，但敏感数据会被监管划出。去中心化不会成为主流形态，但开放协议、可验证身份、可携带记忆格式等部件会约束大厂。

来源：memx · MacPaw · Zep · Stanford HAI · Loyal Agents · ScienceAlert · Layer3 · Coinbase · 凤凰科技 · 网信办

SCENARIOS

08 终局：前台归一、后台垂直

推向归一

用户只想对一个对象说话；记忆有复利；操作系统天然占位。

⇄

推向垂直

专业领域需要深度和资质；超级 App 不会交出交易数据；出事需要明确的责任方。

两股力量的结果是**“一个总管 + 多个专家”**，2026 年已见雏形：小艺可调用 500 多个伙伴 Skill 和 2,000 多个鸿蒙智能体；千问开放平台入驻伙伴超 1,000 家；Cue 支持多个 agent 群聊分工。再加一个维度：**一个记忆，多个设备入口**（手机、车、眼镜、耳机、音箱）。

EXHIBIT 11 **四种终局情景**

A 系统总管

谁赢 苹果、华为、Google **前提** 操作系统拿到足够多的服务接口

迹象：鸿蒙 Agent 亲和架构、Gemini Intelligence

中美都是主力情景之一

B 超级 App 内的 agent

谁赢 微信、支付宝、WhatsApp **前提** 平台守住门

迹象：微信小微、阿宝、Muse 进 WhatsApp

中国更显著

C 独立助理 + 自有硬件

谁赢 OpenAI、Meta、千问、豆包 **前提** 新硬件形成新入口

迹象：OpenAI 设备、Meta 眼镜、千问眼镜

美国更显著

D 开源自托管

谁赢 极客与隐私优先人群 **前提** 端侧模型足够强

迹象：OpenClaw、开放权重模型

长期小众，但约束大厂

更深一层的判断

谁付钱，agent 就为谁服务。

长期看会形成“用户侧 agent”与“平台侧 agent”的对峙。用户侧 agent 替用户读条款、比价、办迁移，这是用户议价能力的真正来源。

可能错在哪里

用户留存和委托意愿可能远低于预期，个人智能体停留在小事上。

模型能力的跳跃可能顺带解决长任务可靠性，削弱“信任基础设施”的重要性。

微信若全面开放，中国格局会向美国靠拢。

重大安全事件可能引发严厉监管，大幅放慢进程。

来源：C114（小艺生态）

EXHIBIT 12 预测看板（置信度为本报告判断）

十条可验证预测

■■■ 高 ■■□ 中 ■□□ 低至中

#	预测 · 验证信号	时间	置信度
01	**字节、阿里、腾讯、华为都推出常驻云端、能代办的个人智能体** 信号：元宝、字节独立助理正式上线	2027 年底前	■■■
02	**主流产品同时具备云端常驻与本地接入** 信号：云端产品普遍开放本地连接	2027 年	■■■
03	**出现跨平台的 agent 身份与委托授权事实标准，由支付网络或大平台主导** 信号：Web Bot Auth 等方案被主要电商采纳	2027–2028 年	■■□
04	**长任务可靠性成为厂商宣传重点，取代单项跑分** 信号：厂商开始披露任务完成率、接管率	2027 年	■■□
05	**头部产品中至少一家把“不卖排序、不接广告”作为核心承诺** 信号：写入产品条款或品牌宣传	2027 年	■■□
06	**个人智能体付费档位进一步分层，大众档价格下探** 信号：各家入门档价格走向	2027 年	■■□
07	**“可验证的 agent”成为大型电商准入门槛，封锁转向有条件开放** 信号：亚马逊是否放开外部 agent	2027–2028 年	■■□
08	**欧盟出现针对 AI 记忆可携带的规则或执法** 信号：数据保护机构的执法或指南	2028 年前	■■□
09	**金融、健康等高风险场景率先出现对 agent 的忠诚或受托义务要求** 信号：监管指引或行业自律标准	2028 年前	■□□
10	**开源自托管保持小众，但持续造成大厂的产品和定价压力** 信号：大厂产品与开源项目的功能对标	持续	■■■

RECOMMENDATIONS · 均为本报告判断

09 对各类参与者的战略建议

EXHIBIT 13 **分角色建议**

模型厂商与 AI 原生应用

没有系统、没有交易生态，如何守住入口?

把信任做成产品力（硬安全边界、可接管、不卖排序）；用开放协议广接服务；审慎下注硬件，优先耳机、眼镜等不与手机正面竞争的形态。

手机操作系统与终端厂商

如何把系统位置变成服务分发权?

推意图框架和 Skill 生态，给开发者说清流量规则；与超级 App 谈有限开放（参考荣耀与微信 A2A）；把端侧记忆做成隐私卖点。

超级 App 与平台

开放会被绕过，封闭会被边缘化。

自建 agent 守入口；对外部 agent 采用“可验证、有条件开放”；警惕一代豆包手机式的对立在舆论和监管上的代价。

智能硬件厂商

硬件会不会被大平台的 agent “管道化”？

先决定做数据源还是自建闭环；主动接入主流 agent 平台换取分发；用持续感知数据建立通用 agent 无法自己生产的价值。

商家与服务方

如何被 agent 选中，又不失去客户关系?

把商品与服务做成 agent 读得懂的结构化描述；接入可信 agent 验证；部署商家侧 agent；只做合规的 GEO，远离“数据投毒”。

创业者

大厂全面进场后，空间在哪?

聚焦信任基础设施（agent 身份、审计、注入防护、记忆可携带）、高门槛垂直专家 agent、用户侧 agent；避开与大厂正面竞争通用入口。

投资者

哪些环节的价值会沉淀?

关注常驻算力成本曲线、委托深度类指标、协议与验证层的网络效应；对依赖 GUI 绕过平台的模式保持谨慎。

政策制定者

如何在创新与用户保护之间平衡?

优先推动 agent 身份、委托授权和记忆可携带的标准；在高风险场景明确忠诚义务与责任分配；参考携号转网与开放银行的经验。

下一阶段的赢家，不是参数最大的模型，而是用户最敢托付的那一个。

附录

A 待核实事项

以下数据目前仅有单一或二手来源，引用前建议核对原始出处。

- ☐ 亚马逊封禁 Muse 及沃尔玛误拦的细节
- ☐ Gemini Spark 下放到 19.99 美元套餐
- ☐ OSWorld 2.0 论文数据（arXiv:2606.29537）
- ☐ AI 旅行规划调研（66.2% / 15.2%）的原始报告
- ☐ Muse Spark “贡献者”档的官方说明
- ☐ 字节独立助理的产品名与上线时间
- ☐ 个保法第 45 条配套转移条件的现行正式规定

B 术语

MCP	模型上下文协议，让 agent 连接外部工具与服务的开放协议
A2A	agent 与 agent 之间通信的开放协议
UCP/AP2/ACP	Google 的通用电商协议、agent 支付授权协议，以及 OpenAI 与 Stripe 的 agent 电商协议
GUI agent	通过识别屏幕界面、模拟点击来操作应用的 agent
提示注入	在网页或文档中藏入恶意指令，诱使 agent 违背用户意愿
GEO	生成式引擎优化，让内容更容易被 AI 引用和推荐

C 主要来源

各页页脚列出该页来源；完整来源见底稿 Personal Agent 专题研究：问题框架与产业链地图。

Meta 推出个人 agent Muse · Jamaica Gleaner

Gemini Spark · The Next Web

豆包手机“转正” · 蓝鲸

HarmonyOS 7 小艺 · C114

AI 入口开始收费 · 投中网

Designing Loyalty · 斯坦福 HAI

拟人化互动服务管理暂行办法 · 新华网

OpenAI 发布 Dots · ProPakistani

Muse 的安全设计 · The Batch

千问加速打造 Personal Agent · 爱范儿

电脑操作 agent 评测解读 · youngju.dev

网站为何拦截 AI agent · TechCrunch

欧盟《数据法案》云迁移 · Lindahl

“清朗·整治 AI 应用乱象” · 网信办

PERSONAL AGENT · 2026

代理人时代

数据截至 2026 年 10 月。带“本报告判断”字样的内容为分析结论，而非事实。