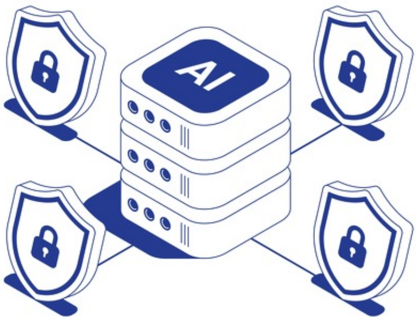
INNOVATION PARTNERSHIPS
UNIVERSITY OF MICHIGAN

MAISON

TECHNOLOGY NUMBER: 2025-022



Technology ID

2025-022

Category

Software

Software & Content

Accelerate Blue Foundry - 2025/Physical Sciences

Inventor

Zaid Ghazal

Further information

Ashwathi Iyer

ashwathi@umich.edu

View online

Accelerate Blue Foundry - 2025 (Physical Sciences)

OVERVIEW

Maison is a real-time, on-device system that scans user prompts—across text, audio, and visual formats—to detect and handle sensitive information before it reaches cloud-based AI models, offering organizations fine-grained control through configurable blocking, warning, or masking actions—thereby bridging the gap between powerful cloud AI and stringent data privacy. Its key value lies in enabling secure adoption of generative AI without relinquishing control over sensitive data.

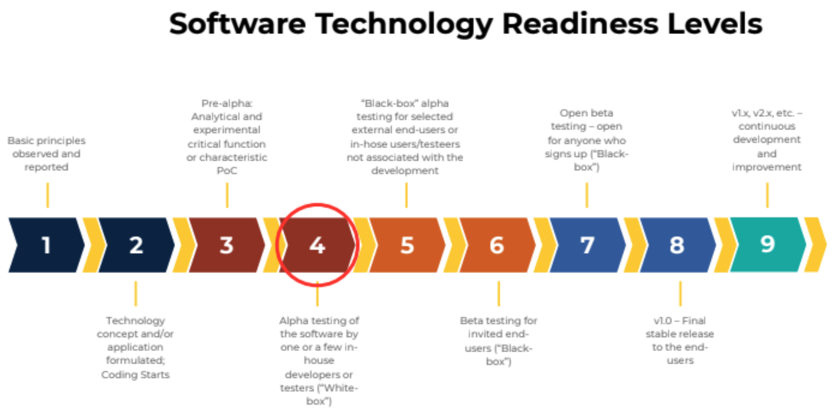
DESCRIPTION

Maison sits between the user and any large language model (LLM), instantly analyzing prompts for sensitive information before any data travels over the network. Unlike other solutions, Maison can handle multiple data types (text, images, audio), operates locally for fast, private detection, and allows organizations to customize what counts as “sensitive” as well as what protective action is taken for each type. Instead of bluntly blocking or encrypting data (which often breaks AI workflows), Maison can intelligently mask sensitive portions while keeping the rest of the prompt intact, so AI tools remain useful without leaking confidential details. This hybrid approach means organizations can benefit from advanced cloud AI without ceding control to an outside vendor.

VALUE PROPOSITION

- **On-premises data control with seamless cloud AI use:** Keep organizational data private and secure without sacrificing access to high-performance cloud generative AI.
- **Highly flexible, multi-format protection:** Detect and manage sensitive data not just in text, but across audio and visual content, with customizable rules and actions per organization.
- **Innovative masking that preserves usability:** Mask sensitive details rather than removing or encrypting them, allowing prompts to maintain context and utility when interacting with AI systems.

TECHNOLOGY READINESS LEVEL


Software Technology Readiness Levels
1
Basic principles observed and reported
2
Technology concept and/or application formulated; Coding Starts
3
Pre-alpha: Analytical and experimental critical function or characteristic PoC
4
Alpha testing of the software by one or a few in-house developers or testers ("White-box")
5
"Black-box" alpha testing for selected external end-users or in-hose users/testeers not associated with the development
6
Beta testing for invited end-users ("Black-box")
7
Open beta testing – open for anyone who signs up ("Black-box")
8
v1.0 – Final stable release to the end-users
9
v1.x, v2.x, etc. – continuous development and improvement

INTELLECTUAL PROPERTY STATUS

Provisional Patent Application pending.

MARKET OPPORTUNITY

With the widespread adoption of generative AI in regulated sectors such as healthcare, finance, legal, and enterprise IT, organizations urgently need tools that protect confidential information without limiting their use of powerful AI services. Maison's ability to provide flexible, real-time data governance unlocks large-scale AI deployments in privacy-conscious industries, compliance-driven organizations, and any enterprise concerned with data leakage (PII, financial data, intellectual property, etc.).

According to Gartner, over 50% of enterprises cite data privacy as their top barrier to AI adoption, underscoring a large, rapidly growing demand for solutions like Maison.

- This project has participated in Customer Discovery

Explore other available products test at University of Michigan