e><change po:nt

<Bots in Chats>

April 29, 2026

Hanna Barakat & Archival Images of AI + AIxDESIGN / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

<Thought experiment>

Agentic AI in contexts with the highest confidentiality and security bar: E2EE and encryption at rest. Is it compatible?

The two endnesses

<AI in E2EE>

Widespread integration of AI in E2EE systems raises serious security concerns.

Analysis on two fronts: (1) the integration of AI assistants within E2EE applications, and (2) the use of E2EE data for training AI models.

<Privacy AI>

More privacy is a win.

Fundamental tension between the guarantees of end-to-end encryption and the delegated authority required for agentic functionality, where “no third-party access” is difficult to reconcile.

Relies heavily on trusted hardware.

<in encrypted systems augmented by AI agents, can control remain with the user?>

<Key design questions>

- Training
- Processing, inference, compute
- Location of the model eg, on/off device
- Permissions and capabilities
- Initiating modes
- Initiating users vs non-initiating users
- Shared user controls
- “Unofficial” clients or agents
- Verifiable execution
- Punching out— what is a TEE?
- First- and third-party integrations
- Interoperability