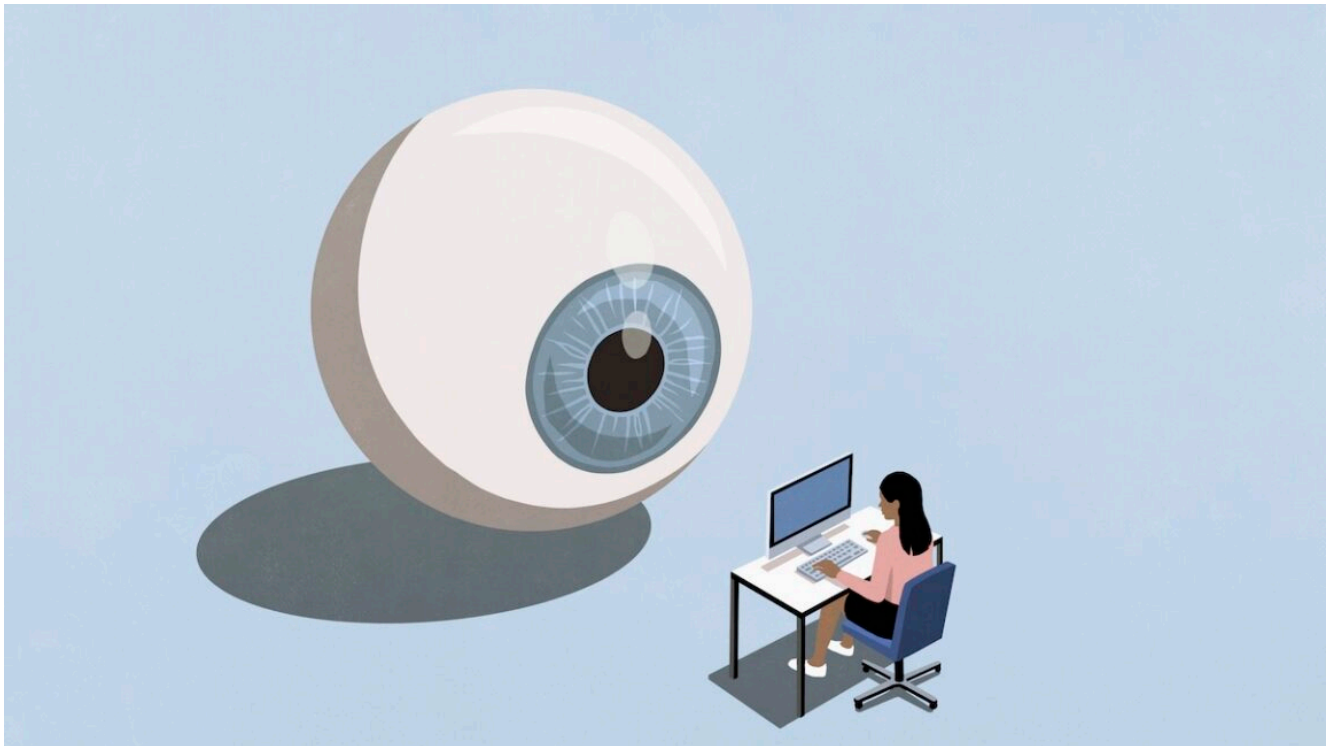


Signal creator Moxie Marlinspike wants to do for AI what he did for messaging



On Confer, remote attestation allows anyone to reproduce the bit-by-bit outputs that confirm that the publicly available proxy and image software—and only that software—is running on the server. To further verify Confer is running as promised, each release is digitally signed and published in a transparency log.

Native support for Confer is available in the most recent versions of macOS, iOS, and Android. On Windows, users must install a third-party authenticator. Linux support also doesn't exist, although this extension bridges that gap.

There are other private LLMs, but

none from the big players

Another publicly available LLM offering E2EE is Lumo, provided by Proton, a European company that's behind the popular encrypted email service. It adopts the same encryption engine used by Proton Mail, Drive, and Calendar. The internals of the engine are considerably more complicated than Confer because they rely on a series of both symmetric and asymmetric keys. The end result for the user is largely the same, however.

Once a user authenticates to their account, Proton says, all conversations, data, and metadata is encrypted with a symmetrical key that only the user has. Users can opt to store the encrypted data on Proton servers for device syncing or have it wiped immediately after the conversation is finished.

A third LLM provider promising privacy is Venice. It stores all data locally, meaning on the user device. No data is stored on the remote server.

Most of the big LLM platforms offer a means for users to exempt their conversations and data for marketing and training purposes. But as noted earlier, these promises often come with major carve-outs. Besides selected review by humans, personal data may still be used to enforce terms of service or for other internal purposes, even when users have opted out of default storage.

Given today's legal landscape—which allows most data stored online to be obtained with a subpoena—and the regular occurrence of blockbuster data breaches by hackers, there can be no reasonable expectation that personal data remains private.

It would be great if big providers offered end-to-end encryption protections, but there's currently no indication they plan to do so. Until then, a handful of smaller alternatives will keep user data out of the ever-growing data

lake.

<https://arstechnica.com/security/2026/01/signal-creator-moxie-marlinspike-wants-to-do-for-ai-what-he-did-for-messaging/>