



Is Your Chatbot **Actually Private?**

"Feels private" is not the same as "is private." What you tell a general-purpose AI chatbot isn't always private. Single-use or specific-use chatbots are more narrowly built, but the same questions apply. Here's how to check!

WHAT YOU TYPE

Every message. At many frontier AI companies, your conversations may be used to train future models by default, and you have to opt out. Single-use or specific-use chatbots are more narrowly trained, so check the privacy policy to learn more about how your chats may be used or shared. You can usually find the privacy policy in the website footer.

WHO YOU ARE

Email, phone, payment info, account ID. These may be linked to everything you say.

HOW YOU USE IT

When you log in, how often, what device, your location. This could be enough to identify you if your chats become public, or if unique information about you is used to train the model and that information becomes available to other users.

WHAT IT FIGURES OUT

Systems make guesses about your mental state, mood, relationships, and health. Stored on company servers, and in real breaches, exposed publicly.

*Developed in partnership with the **AI Mental Health Collective** and Luigi Maruani, Kira Weidner, Carla Geenen, Brigitte Viljoen, Alexis Hernandez-Hons, Jessa Monroe, and Rachel Wood*

THE P·R·I·V·A·T·E FRAMEWORK

P Privacy

Can you actually read it? Many privacy documents were unclear about what rights users actually have over their data. If you can't tell what you're agreeing to, that might be on purpose.

R Retention

How long is your data kept? If you stop using an app or service for good, consider deleting your data. What isn't stored cannot be leaked. Many services have an option to download your data before you delete it.

I Install Permissions

What does the app ask for? Apps may ask for things they don't need: contacts, photos, location, microphone. Say no to anything that isn't necessary for the app to function.

V Vendors

Who else sees your data? Hosting companies, analytics firms, payment processors, advertisers. For apps designed to support mental health or wellbeing, there is a lot of sensitive personal information gathered. Your information may not stay with the app.

A Ads & Training

Is the app free because of ads or training? Then your selling your data may be how the app makes money.

T Transit & breaches

Is your data encrypted, and what happens when something leaks? Even big-name AI companies have accidentally leaked private chats publicly. Assume anything you type could end up searchable in the event of a leak.

E Exit

Can you leave cleanly? Account deletion, data download, and opt-out of AI training should each be one click. Watch for terms of agreement that let the company change the rules.

