# What you may not know about talking to AI

AI tools are useful. I use them every day.

But if you're asking an AI about your health, your finances, your legal situation, your relationships — you need to understand what happens to those conversations.

Most people don't.

**That is not *an accident*, but it sure is *a tragedy*.**

## **1** **Your conversations are not private by default**

When you type something into an AI chatbot, most providers can use that conversation to train their next model.

That means your words — your medical fears, your financial questions, your family conflicts — can become part of a system that millions of other people interact with.

Every major AI provider now operates on an **opt-out** model. If you didn't go looking for a privacy toggle, you're *opted in*.

**The setting exists.**
**But do *you* know where to find it?**

## **2** **Paying doesn't protect you**

This is the most common misconception.

People assume that if they're paying $20/month for a premium AI subscription, their data is private.

**It's not.**

Paid consumer plans — across the industry — generally train on your data by default, just like free plans. The only tiers automatically excluded are enterprise and business accounts.

Your subscription buys you faster responses and better models. **It does not buy you privacy.**

**3** **Opting out doesn't undo what's already done**

Even if you find the privacy toggle and turn it off today, anything you've already shared may have been used.

**You can't un-train a model.** The data is baked in.

What you *can* do is stop future conversations from being included. That's worth doing, but every day you wait is another day of exposure.

Even after you opt out, most providers retain your data for **30 days to 5 years** for safety, legal, or abuse-monitoring purposes.

## **4** **AI is now embedded in tools you already use**

This isn't just about chatbots anymore.

AI is being integrated into:

◆ Your email client

◆ Your messaging apps

◆ Your phone's operating system

◆ Your photo library

◆ Your search engine

◆ Your social media feeds

Many of these features scan your private content to generate suggestions. The line between on-device and cloud processing is **often unclear — and rarely explained**.

## 5 The people most at risk are the least protected

An elderly person asking AI for help understanding a medical bill.

A domestic violence survivor using AI to draft a protective order.

A veteran asking AI to help navigate a benefits claim.

A first-generation student asking AI to help with financial aid applications.

**These people are sharing the most sensitive information imaginable — and they are the least likely to know a privacy setting exists.**
**That's a design failure, which makes it a user problem.**

## What you can do right now

✗ Don't share sensitive personal information with any AI unless you've confirmed how that data is used and retained.

✓ Open every AI tool you use. Find the privacy or data settings. Turn off anything that says your data can be used to "train" or "improve" the model.

✓ Treat AI conversations like **postcards, not sealed letters.** Assume they can be read.

✓ Use incognito or temporary chat modes for anything sensitive.

✓ **Help someone in your life who wouldn't think to do any of this.** That's the most important one.

# Be the person who shows someone else.

AI can be a powerful tool for people who've been failed by institutions — if they can use it safely.

Misalignment between *the price you pay* and *the price you're told you pay* is institutional betrayal in practice.

✉ Share this with someone who needs to see it.

◆ **Apostolos Stamenos, MS**
Technologist for the institutionally betrayed