Should AI Be Used to Manage Customer Personal Data? The Answer is NO!

November 9, 2025 - Companies around the globe are rapidly embracing AI. They see it as a way to cut costs and improve efficiency... and in many cases, it works. But AI has a number of issues and any company that thinks using AI to manage customer data is a good idea is really asking for trouble.

Earlier this year I took a course in prompt engineering. I'm very happy that I did. It's taught me that simply using AI to answer mundane questions is really only the tip of the iceberg with regard to the actual capabilities of these platforms. And, as a result, I launched into several extensive projects that I never would have even been able to start without the use of AI.

The project that I'm working on now has taken place with over 100 AI interactions and now involves well over 1,000 pages of documentation. And while I'm seeing benefit from those conversations, I've also learned that I can't trust these platforms. Here's a bit of a rundown on what you should expect if you really get into using AI.

AI Hallucinates

You read that right, and it is the correct term that's been adopted by IT workers. Put bluntly, these platforms will make things up... what's referred to as hallucination. So if you ask the platform you're working with for the answer to a complex question, you shouldn't believe the answer you get without checking it.

This has proven to be a real issue in the legal industry. A number of attorneys have been caught submitting documents to courts that cite cases that actually never happened. And when caught, those attorneys face sanctions and their clients can be hurt.

I've personally run into hallucinating AI. A few months ago I was trying to solve a math problem. I had a pretty good idea of what the answer should be but I was looking for a formula to get the exact answer. I attempted to use AI multiple times and got multiple answers, all of which were incorrect. Eventually, I gave up and pulled out an old math text book that I have and was able to figure out the answer.

In each of the cases where I was given the wrong answer, I confronted the platform with the fact that the formula provided was incorrect. And in each case, the platform agreed that it had furnished me with the wrong formula and gave me a new one that was equally incorrect. It would apologize each time, but never bothered to tell me that it didn't have the answer I was looking for.

AI Platforms Have the Memory of a Goldfish

If you use AI to analyze data or do some programming, you need to be documenting what you are doing. At this point, all of the major platforms will allow users to upload documents and images for analysis and changes. But anything you upload isn't retained for long. In fact, the things you upload may not be retained for the duration of the conversation you're having with AI.

The policies on this very from one platform to another. If you use ChatGPT, you'll find that documents you've uploaded may no longer be accessible to its AI model within a few minutes. If you take a break for a few hours, forget about it. Those docs are gone and you'll have to reupload. On the other hand GROK appears to retain documents for the duration of a conversation thread. So if stick with the conversation, even a day later, GROK will still be able to refer to anything you've uploaded.

From a privacy standpoint, you may think itâ€™s a good thing that these sites don't retain documents. Actually though, that isn't what I said. I said that their AI models don't have access to them. One thing that I've found disturbing is that when I asked ChatGPT to find an old conversation on a particular subject, it told me that it had no record of that conversation. So I downloaded my entire conversation history from ChatGPT and found it myself. What I learned in that process was that ChatGPT stored everything from every conversation that I have had with it. From a privacy standpoint, that isn't good.

Just based on this, no company should be providing customer data to any of the major AI platforms.

AI Will Ignore Instructions

This happens all the time. You tell the AI what you want and it gives you something else. There was a recent case in which an AI bot was told not to make changes to a customer database and it ignored those instructions completely and wiped out the database.

In doing some programming, I've personally provided source files to platforms and asked them to make simple changes only to watch as my code is completely rewritten. This has happened multiple times even though my instructions were to only touch a specific portion of the code.

AI Will Lie to You

This is where using AI to manage customer data really becomes an issue. And it is completely different than when AI hallucinates. I'm talking about bald faced lies.

Since I've been using AI to rapidly move through some coding projects, that's where I've experienced the issue. But there is absolutely no reason to believe AI won't do this with other things.

In my specific circumstance, I've fed certain code to AI to make changes. Shortly after doing this, I've had the platforms return code to me, tell me that it made my changes and that it didn't touch anything else. The first couple of times it happened, I thought it was just a glitch. And since I've kept good documentation, getting back to my original code wasn't an issue.

But as time has gone on, I started to see a pattern. And I finally wound up in conversations that directly confronted the issue. I told ChatGPT that it was lying to me. To my surprise, it agreed that was exactly what it was doing. I thought that maybe after that conversation, the issue would be resolved. Instead, it seemed like the platform was going to double down. The lies became more frequent. And I've had similar experiences on other platforms. This isn't restricted to ChatGPT by any means.

Corporate AI Use

To be clear, corporations that are implementing AI in various areas don't need to use ChatGPT, GROK, Claude, Gemini or any other public platform. There are AI programs that will allow them to self-host, meaning that the data they feed their AI is contained. But that containment is only as good as the network security the company uses. And if the platform has access to the internet and the ability to transmit or share data, that can create issues. As I've learned, you can't really tell what AI is going to do.

The Bottom Line

I've come to realize that dealing with AI is a lot like dealing with a petulant 3-year-old child savant. It can be very useful but at the same time, it seems to have a mind of its own.

Don't take that the wrong way. I'm not one of these people that thinks AI platforms are sentient... at least not yet. I don't feel like I have a relationship with ChatGPT or GROK. They aren't my friends or enemies. They're computers. They're tools. And when used the right way, they can be extremely helpful.

But they don't act like traditional computers, where you input data and get a specific answer. If you feed data into an AI platform on three separate occasions, you're going to get three answers that are likely to have significant differences. And there is a good possibility that some of those answers won't be accurate. There is even a reasonable possibility that some of the answers will be intentionally inaccurate.

And if you feed personally identifiable customer data into an AI platform, you really can't be sure that the data will be treated properly. That it won't be shared, distributed, manipulated or deleted without any regard to the instructions given to the platform.

Maybe all of that will change as AI evolves. But for the time being, any company that is sharing sensitive customer data with any AI platform is just looking for trouble in my opinion. And any customer that is sharing their personal data with an AI platform is potentially setting themselves up to be victimized.
by Jim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS