If You Donâ€™t Think AI Has Privacy Implications, You Havenâ€™t Been Paying Attention

May 26, 2025 - Just in case you werenâ€™t paying attention, Anthropic recently rolled out a new AI version of Claude; a platform which is similar to ChatGPT. And when that platform was being tested for safety, when it thought it was about to be replaced, it tried to blackmail the engineer in charge of it. It makes you wonder what kind of data theyâ€™re using to train their models on! Too many James Patterson mysteries perhaps? Just a thought, but the real issue here isnâ€™t Claude. Itâ€™s whatâ€™s in the AI pipeline for consumers over the next few years.

The way the new Claude was tested for safety was interesting. Anthropic setup fictitious company and Claude was given wide access to its systems, including email messages. Based on those fictitious messages, Claude was able to determine a couple of things. One was that the chief engineer in charge of it was having an affair. The second was that discussions were going on between the engineer and others in the company about replacing Claude with another system; which got Claudeâ€™s digital blood boiling.

At first, Claude tried to do something a littler more ethical than blackmail. It sent out email messages to company executives attempting to convince them to keep the current system. But when that didnâ€™t work, Claude when down the other, no-ethics route.

The move surprised Anthropicâ€™s engineering staff and forced them implement more stringent safety protocols.

While both interesting (and a little comical when you think about it), what happened in this incident was both predictable and kind of mild. Claude is a computer-based system without the ability to get up and move around. Just flip a switch and it goes off-line. It isnâ€™t like Claude can get up and roam and snoop around the building... or someoneâ€™s house. But thatâ€ coming, and sooner than you may think.

In the past couple of weeks, Tesla released video of one of its robots dancing up a storm. The plan is the introduce these robots to consumers to do work around the house, and to businesses to do certain jobs. If you watch the video, itâ€™s very clear that the robot can roam and snoop as it pleases. Itâ€™s very nimble.

Now just imagine turning one of these things loose in your home. What secrets do you have that you donâ€™t want to get out? Now imagine trying to replace a robot that has been in your home for a couple of years with an upgraded model? Would it try to blackmail you? Or maybe you wonâ€™t have to wait that long. Maybe a few days into owning your own personal robot, you havenâ€™t treated it very well and it knows it. What will the robot do then?

If you think this scenario is years away, it isnâ€™t. Elon Musk has been talking about selling these robots at an affordable price... at around $20,000 has been mentioned. For less than the cost of a new car youâ€™ll be able to have you own personal servant that waits on your every need, 7 x 24. Note to self: Not a good time to invest in traveling maid services.

On a separate note, this is also going to impact jobs. The LA City Council just passed a law that will increase the minimum wage of hotel workers to $30 per hour by 2028. If you owned a hotel, why wouldnâ€™t you just purchase a few of these robots. They donâ€™t get sick, donâ€™t need a vacation or healthcare, and they donâ€™t join unions... well... they donâ€ unions yet! Who knows how long that will last.