This journalist's Otter.ai scare is a reminder that cloud transcription isn't completely private

A report recently published by *Politico* about the automated transcription service Otter.ai serves as a great reminder of how difficult it can be to keep things truly private in the age of cloud-based services. It starts off with a nerve-wracking story – the journalist interviewed Mustafa Aksu, a Uyghur human rights activist who could be a target of surveillance from the Chinese government. But though they took pains to keep their communication confidential, they used Otter to record the call – and a day later, they received a message from Otter asking about the purpose of the conversation with Aksu.

Obviously, it was a concerning email. After receiving mixed messages from an Otter support agent about whether the survey was real or not, the reporter went down a rabbit hole trying to figure out what had happened. He details his dive into the service's privacy policy (which does let Otter share some info with third parties), and lays out how the ease and utility of transcription software can override critical thinking about where potentially sensitive data is ending up.

"Hey Phelim, to help us improve your Otter's experience, what was the purpose of this particular recording with titled 'Mustafa Aksu'"
It's an important wake up call – automated transcription

services are popping up everywhere, both from standalone companies like Otter (which we at *The Verge* have used and recommended) and Trint, and as built-in components of services like Zoom and Google Docs. Rationally, we know that the government can get at data stored by these cloud services with a subpoena, but convenience and accessibility can sometimes make it easy to forget those concerns. As the report says, though:

> *"We have not and would not share any data, including data files, of yours with any foreign government or law enforcement agencies," Otter's Public Relations Manager, Mitchell Woodrow, told me via email. "To be clear, unless we are legally compelled to do so by a valid United States legal subpoena, we will not ever share any of your data, including data files, with any foreign government or law enforcement agencies."*

The report is more of a wake up call than a takedown of a popular service — there's no big reveal that the transcript had been accessed by a nation's spy agency, and Otter told the reporter that Aksu's name was in the survey because it was in the title of the transcription. The company also said that it's stopped doing those kinds of surveys, because of the disconcerting effect they could have.

But the fact that the government can legally get its hands on the information we provide to these services is something worth keeping in mind — especially when it comes to choosing between cloud services and alternatives like apps that use on-device transcription, or offline recorders. Even for those of us not dealing with confidential sources, it's well worth reading a report about these increasingly common transcription tools from someone who does.

https://www.theverge.com/2022/2/16/22937766/go-read-this-otter-ai-transcription-data-privacy-report