JUST TECH

NEWS

My journey down the rabbit hole of every journalist’s favorite app | POLITICO

By Phelim Kine
February 28, 2022

So when I talked to Aksu in November, I made sure to use Signal, an encrypted phone app, to protect our discussion about psychological trauma afflicting Uyghurs overseas.

The next day, I received an odd note from Otter.ai, the automated transcription app that I had used to record the interview. It read: “Hey Phelim, to help us improve your Otter’s experience, what was the purpose of this particular recording with titled ‘Mustafa Aksu’ created at ‘2021-11-08 11:02:41’?”

Three responses were offered: “Personal transcription,” “Meeting or group collaboration,” and “Other.”

I froze. Was this a phishing attack? Was Otter or some entity that had access to Otter’s servers spying on my conversations?
I contacted Otter to verify if this was indeed a real survey or some clever phishing ruse. An initial confirmation that the survey was legitimate was followed by a denial from the same Otter representative, laced with a warning that I “not respond to that survey and delete it.” My communications with Otter were all restricted to email and were sporadic, often confusing and contradictory.

In the three months since that initial exchange (and there was more to come), I’ve gone down the rabbit hole — talking to cybersecurity experts, press freedom advocates and a former government official — to try and understand what vulnerabilities and risks are present in this app that’s become a favorite among journalists for its fast, reliable and cheap automated transcription.

Source: My journey down the rabbit hole of every journalist’s favorite app | POLITICO