Translator Danger: Security Risks of the CoPilot Translator

The world's first microchip translator presents unparalleled cybersecurity and privacy challenges.

By Ty Feeney

Oct. 16, 2020

Tony Webster

The CoPilot device has revolutionized the tourism industry. The amount of international travel, across the entire globe, has nearly doubled. Countries such as Bangladesh, India, and Pakistan have seen international travel skyrocket. New tourism revenue in the third world has lifted millions out of poverty.

But the CoPilot device has hidden drawbacks. For the CoPilot device to continue improving translation quality and keep up with new vocabulary and grammar in hundreds of languages, the CoPilot machine learning engine needs to collect data from both its earpiece and brain chip. Unfortunately, the device's data storage and collection risks user privacy and safety.

Having data on hundreds of millions of users leaves the company vulnerable to cyberattacks. As the device gains prevalence, black hat hackers have more of an incentive to steal its private user data. More hackers will turn towards the CoPilot device over other software because of its vast library of conversations.

With more and more governments, including the US, relying on the CoPilot for translation, hackers could gain access to confidential conversations. CoPilot servers bring data on diplomatic negotiations and top-secret military operations to one convenient target. Hackers can easily sell this data to foreign governments or terrorist organizations, or they can choose to use it to influence public opinion and interfere with the outcome of national elections.

Some supporters of CoPilot argue that cybersecurity concerns should not stop governments from using the revolutionary technology. If the threat of cyberattacks does not stop politicians from using email, instant messaging, and video conferencing, why should the CoPilot raise a concern? But there is false equivalence in this argument: the translation data provided by CoPilot contains vastly more classified information than any other web service. Usually, governments can provide their own technology infrastructure for dealing with top secret information. But CoPilot is not so easily replaceable. CoPilot has a monopoly in the real-time translation market, and no government has developed a translation service that is even remotely as reliable as the CoPilot device. To access even basic digital translation services, government officials must risk putting their most secure data on CoPilot's private servers.

Governments may also use the CoPilot as a tool for spying on their citizens. If American adversaries, such as China or Russia, request data about their citizens, CoPilot will have to oblige, or risk losing almost half of their daily users. China already uses a social credit score to track their citizens, and people with low social credit scores are banned from flights, discriminated in employment, and subjected to public humiliation. If China decides to integrate CoPilot data with their social credit system, Chinese citizens will be punished for what they say in conversations with American family members. And in Russia, a country known for defaming and killing journalists, combining already existing facial recognition with CoPilot's conversation data will lead to even less political speech.

Additionally, CoPilot may start selling private user data to advertisers. At the low price of $89, the CoPilot translator loses millions of dollars a year improving and maintaining their software infrastructure. To encourage further rounds of venture funding or set themselves up for an IPO (Initial Public Offering), CoPilot may resort to selling user data. A slight change to the CoPilot terms and conditions could put your conversations on the open market.

Some reporters will point out that many unprofitable tech firms, such as Uber, Lyft, and Pinterest, have received substantial IPOs despite their unprofitability. Investors continue buying in and subsidizing business costs, despite losses every year. But unlike CoPilot, these companies use subscription or advertisements as a replenishable source of revenue. As a one-time purchase, CoPilot cannot depend on this infinite revenue supply. Eventually, CoPilot's revenue will taper out, and investors will become weary of investing the capital that CoPilot needs to maintain its growth. CoPilot, to stimulate investor funding and keep growing, will inevitably join Google and Facebook in the advertisement market. Once CoPilot starts selling user data, managing and understanding your data becomes even more impossible.

But CoPilot has a far greater ability to harvest user data and control user behavior than any of the social media giants. Researchers have shown that their brain chip, which is meant only to interpret thoughts for translation, can be altered to read information from other parts of the brain, or to write information into the brain. And with no clear uninstallation process, current users have few mechanisms for backing out of their deal with CoPilot. Although CoPilot has almost certainly never used the chip for mind control, the possibility of mass mind control from a multi-billion-dollar corporation raises alarms.

Thus, we should force CoPilot to shut down until they develop better safeguards for protecting user data. Extensive government regulation and new legislation will be needed to keep the CoPilot device safe and secure. Until such time, stop using the CoPilot device, and use a book or a human translator instead. If you already have the device implanted, have the device removed, if possible. A national boycott will give CoPilot, and national regulators, the incentive to protect your data security.