Quanto sono sicuri gli strumenti di trascrizione usati dai giornalisti?

Maria Cattini | 13/05/2023 | Tips tools

Oggi parliamo della sicurezza e affidabilità degli strumenti di trascrizione più utilizzati dai giornalisti.

Caricare l'audio, per esempio, su un servizio di trascrizione significa consegnare una copia di quella registrazione a un'azienda e questo comporta considerazioni di sicurezza.

Il lavoro giornalistico spesso dipende dai servizi di trascrizione per la creazione di registri scritti dell'audio registrato, dall'assistenza nella ricerca alla sottotitolazione di video fino alla pubblicazione di interviste.

Ma caricare l'audio su un servizio di trascrizione significa dare una copia di quella registrazione, a volte sensibile, a un'azienda.

Sebbene non esista un unico servizio che soddisfi tutte le nostre esigenze di privacy dei dati, qui disimballiamo le pratiche di sicurezza e privacy per i servizi di trascrizione più diffusi, valutiamo quando i giornalisti dovrebbero utilizzare i servizi di trascrizione remota ed esploriamo come ridurre al minimo i rischi quando si lavora con audio sensibile.

In un sondaggio informale, al quale hanno partecipato più di 50 giornalisti, sui servizi di trascrizione preferiti ne sono stati selezionati 5: Descript, Otter.ai, Rev, Temi e Trint.

Quanto sono sicuri questi strumenti di trascrizione?

E cosa stanno facendo per proteggere i dati, registrazioni private e trascrizioni?

Descript

Descript afferma nella sua documentazione di sicurezza che, sebbene abbia la capacità tecnica, si impegna a non guardare i dati degli utenti se non in determinate circostanze, ad esempio durante l'elaborazione di voci specifiche generate dal computer o quando un utente ha richiesto una revisione a un rappresentante del servizio clienti.

Gli utenti possono anche scegliere di condividere le informazioni per migliorare il servizio.

Dietro le quinte, Descript utilizza una piccola manciata di servizi per elaborare le trascrizioni. Descript utilizza Google Cloud Speech-to-Text per fornire la trascrizione automatica.

Google cancella i tuoi dati dai suoi server al termine della trascrizione. Secondo la sua documentazione, Descript utilizza anche Rev per fornire la trascrizione automatica o umana.

Descript dice: "Se richiedi una trascrizione di White Glove, condivideremo i tuoi file audio con Rev, che ha stretti accordi di riservatezza con tutti i suoi dipendenti".

Descript offre una potente funzionalità chiamata Overdub, che consente agli utenti di inserire voci realistiche generate al computer nella trascrizione.

A tal fine, Descript utilizza Google Cloud per elaborare e riprodurre la tua voce. Descript genererà campioni " non diffamatori " della tua voce e i revisori umani su Mechanical Turk di Amazon ascolteranno questo campione audio per confermare che suona bene.

Descript afferma che i loro dipendenti possono anche rivedere l'audio caricato, nonché l'audio di output generato dal computer per garantire la qualità.

Non offre l'autenticazione a due fattori.

Otter.ai

Come gli altri servizi di trascrizione qui descritti, Otter.ai crittografa i propri dati sui server Amazon Web Services e conserva le chiavi di crittografia.

La sua politica sulla privacy suggerisce di utilizzare questo accesso per fornire il servizio e per addestrare la sua trascrizione di intelligenza artificiale (AI) con registrazioni audio collettive "de-identificate".

L'informativa sulla privacy di Otter.ai dice: "Solo con la tua esplicita autorizzazione esamineremo manualmente alcune registrazioni audio per perfezionare ulteriormente i nostri dati di addestramento del modello".

Otter.ai dice a Freedom of the Press Foundation in un'e-mail: “Non vendiamo o condividiamo i tuoi dati con terze parti, né accediamo ai tuoi dati senza il tuo esplicito permesso.

Hai anche il pieno controllo per eliminare le tue conversazioni. L'eliminazione di una conversazione la elimina definitivamente dai server di Otter e non può essere annullata.

Il white paper sulla sicurezza dell'azienda afferma che solo due amministratori hanno accesso al suo database "come richiesto dalla loro funzione lavorativa". Il white paper sulla sicurezza di Otter.ai suggerisce che non si basa su servizi di terze parti per elaborare audio o trascrizioni, ma solo per archiviare i dati degli utenti .

L'autenticazione a due fattori è supportata sugli account Business ed Enterprise, gli account Pro gratuiti a pagamento non possono utilizzare questa importante funzionalità di sicurezza.

REV

Rev offre sia la trascrizione automatica che umana. Secondo la documentazione sulla sicurezza di Rev, i dipendenti sono “limitati a gestire i dati necessari per svolgere il proprio lavoro. Il nostro personale è formato sull'uso corretto dei nostri sistemi e sulle migliori pratiche per la sicurezza e la privacy". Tuttavia, le circostanze in cui i dipendenti possono accedere ai dati degli utenti non sono chiare.

Abbiamo contattato Rev per maggiori dettagli, ma non abbiamo ricevuto risposta al momento della pubblicazione. La documentazione sulla sicurezza di Rev suggerisce che non fa affidamento su terze parti per automatizzare la trascrizione, ma si affida invece ai suoi oltre 60.000 trascrittori manuali freelance noti come "Revvers".

Richiede rigorosi accordi di riservatezza e, a seguito di un rapporto del 2019 di OneZero, Rev ora impedisce ai trascrittori di scaricare l'audio dei clienti.

E' l'unico servizio di questo gruppo che offre l'autenticazione a due fattori a tutti gli utenti.

TEMI

Temi è un servizio di trascrizione da audio a testo che utilizza un software avanzato di riconoscimento vocale. Temi è gestito da Rev, motivo per cui i due servizi hanno politiche sulla privacy praticamente identiche e proprietà di sicurezza simili. Temi non sembra utilizzare alcun servizio di elaborazione di terze parti. A differenza di Rev, Temi non offre trascrizioni umane e afferma sul suo sito Web : "I file vengono trascritti da macchine e non vengono mai visti da un essere umano".

Non offre l'autenticazione a due fattori.

TRINT

Trint è un servizio di trascrizione basato sull'intelligenza artificiale per file audio e video, popolare tra i videografi perché si integra con l'editor video Adobe Premiere Pro, oltre ad alcune altre funzionalità.

La documentazione di Trint è chiara sulle sue misure di sicurezza. Ha la capacità di decrittografare la trascrizione e i dati audio degli utenti, anche se si impegna affermativamente a non farlo se non in casi insoliti e solo con il consenso scritto di un cliente .L' informativa sulla privacy della piattaforma di Trint afferma che si basa su MongoDB Atlas, un database cloud. Mentre i dipendenti di MongoDB possono accedere tecnicamente ai dati caricati su Trint, il servizio di database cloud ha politiche e controlli per limitare tale accesso a un piccolo gruppo di ingegneri, "solo per garantire l'affidabilità del servizio".

Trint utilizza anche un servizio chiamato Transloadit, che aiuta a caricare ed elaborare file. Transloadit si impegna a archiviare i file elaborati per 24 ore prima di eliminarli, aggiungendo: “I dipendenti di Transloadit esaminano i tuoi file solo per risolvere i problemi. Questo accade raramente e, quando accade, lo facciamo con la consapevolezza che tutto ciò che vediamo deve essere mantenuto strettamente confidenziale". Trint non offre l'autenticazione a due fattori.

Il consiglio è quello di evitare del tutto la trascrizione del tuo audio in mani sbagliate. Potrebbe mettere a rischio le persone!

Tuttavia, ci sono alcune situazioni in cui un servizio di trascrizione è una scelta necessaria o più facile, come quando si trascrive un'intervista che verrà pubblicata per intero. Poiché questi servizi di solito hanno accesso all'audio e alle trascrizioni, i giornalisti devono comunque prendere decisioni soggettive su quando condividere file con un servizio di trascrizione.

A cui pensare prima di caricare:

- Intendi pubblicare questa trascrizione in un luogo pubblico?
- Quanto è sensibile questo audio/trascrizione?
- Ti *sei* impegnato a mantenere riservato questo audio/trascrizione?
- Quanto ti senti a tuo agio con un trascrittore umano che ascolta l'audio, al contrario di uno strumento di riconoscimento vocale automatizzato?
- Alcuni servizi di trascrizione basati sul riconoscimento vocale automatico (es. Trint) si impegnano a *non* guardare le tue trascrizioni. Queste assicurazioni sono abbastanza ragionevoli per questo particolare audio/trascrizione?
- Allo stesso modo, molti servizi (ad es. Rev) che offrono trascrizionisti umani richiedono anche che tali trascrizionisti firmino accordi di riservatezza e/o non divulgazione. Queste assicurazioni sono abbastanza ragionevoli per questo particolare audio/trascrizione?
- Molti servizi di trascrizione dipendono da terze parti per l'elaborazione della trascrizione. Le terze parti che hanno accesso all'audio sono accettabili per questo particolare file?
- Il tuo account con il servizio memorizza audio o trascrizioni particolarmente sensibili? Quali garanzie hai dalla piattaforma per mantenere sicuro il tuo account?

Qualunque servizio si scelga, è necessario dare un'occhiata alla sua documentazione di sicurezza per assicurarci che non ci siano sorprese indesiderate.