**THERE’S A CHANCE** that [ChatGPT](https://www.wired.com/story/how-chatgpt-works-large-language-model/) knows personal details about you—and if it doesn’t, it might just make something up. As OpenAI’s generative text chatbot has [boomed in popularity over the past six months](https://www.wired.com/story/chatgpt-api-ai-gold-rush/), the risks of the system being trained on data vacuumed up from the web have become clearer.

Data regulators around the world are investigating issues with how OpenAI gathered the data it uses to train its large language models, the accuracy of answers it provides about people, and other legal concerns about the use of its generative text systems. Europe’s data regulators have [joined forces to look at OpenAI](https://www.politico.eu/article/european-data-regulators-set-up-chatgpt-taskforce/) after Italy temporarily [banned ChatGPT from the country](https://www.wired.com/story/italy-ban-chatgpt-privacy-gdpr/). And [Canada is also investigating the technology’s potential privacy risks.](https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023/an_230404/)

In Europe, [GDPR laws](https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018) require companies and organizations to demonstrate lawful reasons for handling people’s personal information and to let people access information about them, be informed of how their information is used, and demand that errors be rectified. In some cases, they can ask that certain types of data be erased. The way people’s [personal information has been used in training data](https://www.wired.com/story/italy-ban-chatgpt-privacy-gdpr/) has been an early area of concern for EU regulators.

As people have experimented with the chatbot, asking it questions about their lives and friends, a range of potential problems have emerged. OpenAI warns that ChatGPT may provide inaccurate information, and people have found that it makes up jobs and hobbies. It has [cooked up false newspaper articles](https://www.theguardian.com/commentisfree/2023/apr/06/ai-chatgpt-guardian-technology-risks-fake-article) that had even the alleged human authors wondering if they were real. It generated incorrect statements saying a law professor was [involved in a sexual harassment scandal](https://www.washingtonpost.com/technology/2023/04/05/chatgpt-lies/), and it said a mayor in Australia had been [implicated in a bribery scandal](https://www.theguardian.com/technology/2023/apr/06/australian-mayor-prepares-worlds-first-defamation-lawsuit-over-chatgpt-content)—he is preparing to sue for defamation.

It’s not just individuals who are concerned about how data is used. Samsung has banned employees from using generative AI tools, in part over fears about how data is stored on external servers and the risk that [company secrets could ultimately be disclosed to other users](https://www.bloomberg.com/news/articles/2023-05-02/samsung-bans-chatgpt-and-other-generative-ai-use-by-staff-after-leak). (There are separate issues around [copyright](https://www.lexology.com/pro/content/openai-fights-back-against-copyright-infringement-data-claims) and intellectual property.)

In response to the scrutiny—particularly from the Italian data regulator, which has now allowed ChatGPT back into the country [after OpenAI made changes to its service](https://www.gpdp.it/home/docweb/-/docweb-display/docweb/9881490#english)—the company has introduced tools and processes that allow people more control over at least some of their data. Here’s how to use them.

**Get Your Data Removed From ChatGPT**

ChatGPT and [GPT-4](https://www.wired.com/story/gpt-4-openai-will-make-chatgpt-smarter-but-wont-fix-its-flaws/) generate their human-like answers statistically—predicting which words are likely to follow others after seeing millions of examples of sentences written by human authors. OpenAI has been secretive about the data it has trained its [large language models on](https://www.wired.com/story/how-chatgpt-works-large-language-model/), so nobody outside the company knows exactly how much of the web (including people’s personal information) it has scraped in the process.

OpenAI says its large language models are trained on three sources of information: data taken from the web, data that the company licenses from others, and the information people feed it through chats. This can include information about individuals. “A large amount of data on the internet relates to people, so our training information does incidentally include personal information,” OpenAI explains in a [post](https://help.openai.com/en/articles/7842364-how-chatgpt-and-our-language-models-are-developed), stating that it takes steps to reduce the amount it gathers.

OpenAI has now introduced a [Personal Data Removal Request form](https://share.hsforms.com/1UPy6xqxZSEqTrGDh4ywo_g4sk30) that allows people—primarily in Europe, although also in Japan—to ask that information about them be removed from OpenAI’s systems. It is described in an OpenAI blog post about how the company [develops its language models](https://help.openai.com/en/articles/7842364-how-chatgpt-and-our-language-models-are-developed).

The [form](https://share.hsforms.com/1UPy6xqxZSEqTrGDh4ywo_g4sk30) primarily appears to be for requesting that information be removed from answers ChatGPT provides to users, rather than from its training data. It asks you to provide your name; email; the country you are in; whether you are making the application for yourself or on behalf of someone else (for instance a lawyer making a request for a client); and whether you are a public person, such as a celebrity.

OpenAI then asks for evidence that its systems have mentioned you. It asks you to provide “relevant prompts” that have resulted in you being mentioned and also for any screenshots where you are mentioned. “To be able to properly address your requests, we need clear evidence that the model has knowledge of the data subject conditioned on the prompts,” the form says. It asks you to swear that the details are correct and that you understand OpenAI may not, in all cases, delete the data. The company says it will balance “privacy and free expression” when making decisions about people’s deletion requests.

Daniel Leufer, a [senior policy analyst](https://twitter.com/djleufer) at digital rights nonprofit Access Now, says the changes that OpenAI has made in recent weeks are OK but that it is only dealing with “the low-hanging fruit” when it comes to data protection. “They still have done nothing to address the more complex, systemic issue of how people’s data was used to train these models, and I expect that this is not an issue that’s just going to go away, especially with the creation of the [EDPB taskforce on ChatGPT](https://edpb.europa.eu/news/news/2023/edpb-resolves-dispute-transfers-meta-and-creates-task-force-chat-gpt_en),” Leufer says, referring to the European regulators coming together to look at OpenAI.

“Individuals also may have the right to access, correct, restrict, delete, or transfer their personal information that may be included in our training information,” OpenAI’s [help center page also says](https://help.openai.com/en/articles/7842364-how-chatgpt-and-our-language-models-are-developed). To do this, it recommends emailing its data protection staff at dsar@openai.com. People who have already requested their data from OpenAI [have not been impressed with its responses](https://www.linkedin.com/posts/alexanderhanff_openai-cease-and-desist-letter-activity-7054088690901409792-2LXI/). And Italy’s data regulator says [OpenAI claims it’s “technically impossible”](https://www.gpdp.it/home/docweb/-/docweb-display/docweb/9881490" \l "english" \t "_blank) to correct inaccuracies at the moment.

**How to Delete Your ChatGPT Chat History**

You should be cautious of what you tell ChatGPT, especially given OpenAI’s limited data-deletion options. The conversations you have with ChatGPT can, by default, be used by OpenAI in its future large language models as training data. This means the information could, at least theoretically, be reproduced in answer to people’s future questions. On April 25, the company introduced a [new setting to allow anyone to stop this process](https://openai.com/blog/new-ways-to-manage-your-data-in-chatgpt), no matter where in the world they are.

When logged in to ChatGPT, click on your user profile in the bottom left-hand corner of the screen, click **Settings**, and then **Data Controls**. Here you can **toggle off Chat History & Training**. OpenAI [says](https://help.openai.com/en/articles/7730893-data-controls-faq) turning your chat history off means data you input into conversations “won’t be used to train and improve our models.”

As a result, anything you enter into ChatGPT—such as information about yourself, your life, and your work—shouldn’t be resurfaced in future iterations of OpenAI’s large language models. OpenAI says when chat history is turned off, it will retain all conversations for 30 days “to monitor for abuse” and then they will be permanently deleted.

When your data history is turned off, ChatGPT nudges you to turn it back on by placing a button in the sidebar that gives you the option to enable chat history again—a stark contrast to the “off” setting buried in the settings menu.

**HAY UNA OPORTUNIDAD** que  [ChatGPT](https://www.wired.com/story/how-chatgpt-works-large-language-model/) conoce detalles personales sobre usted, y si no es así, podría inventar algo. A medida que el chatbot de texto generativo de OpenAI ha  [ganado popularidad en los últimos seis meses](https://www.wired.com/story/chatgpt-api-ai-gold-rush/) , los riesgos de que el sistema se entrene con datos extraídos de la web se han vuelto más claros.

Los reguladores de datos de todo el mundo están investigando problemas relacionados con la forma en que OpenAI recopiló los datos que usa para entrenar sus grandes modelos de lenguaje, la precisión de las respuestas que brinda sobre las personas y otras inquietudes legales sobre el uso de sus sistemas de texto generativo. Los reguladores de datos de Europa han  [unido fuerzas para analizar OpenAI](https://www.politico.eu/article/european-data-regulators-set-up-chatgpt-taskforce/) después de que Italia  [prohibiera temporalmente ChatGPT en el país](https://www.wired.com/story/italy-ban-chatgpt-privacy-gdpr/) . Y  [Canadá también está investigando los posibles riesgos de privacidad de la tecnología.](https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023/an_230404/)

En Europa,  [las leyes del RGPD](https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018) exigen que las empresas y organizaciones demuestren razones legales para manejar la información personal de las personas y permitan que las personas accedan a su información, estén informados de cómo se usa su información y exijan que se rectifiquen los errores. En algunos casos, pueden solicitar que se eliminen ciertos tipos de datos. La forma en que  [se ha utilizado la información personal de las personas en los datos de capacitación](https://www.wired.com/story/italy-ban-chatgpt-privacy-gdpr/) ha sido un área temprana de preocupación para los reguladores de la UE.

A medida que las personas experimentaron con el chatbot, haciéndole preguntas sobre sus vidas y amigos, surgió una variedad de problemas potenciales. OpenAI advierte que ChatGPT puede proporcionar información inexacta, y las personas han descubierto que inventa trabajos y pasatiempos. Ha  [inventado artículos periodísticos falsos](https://www.theguardian.com/commentisfree/2023/apr/06/ai-chatgpt-guardian-technology-risks-fake-article) que incluso los presuntos autores humanos se preguntaban si eran reales. Generaba declaraciones incorrectas que decían que un profesor de derecho estaba  [involucrado en un escándalo de acoso sexual](https://www.washingtonpost.com/technology/2023/04/05/chatgpt-lies/) , y decía que un alcalde de Australia había estado  [implicado en un escándalo de soborno](https://www.theguardian.com/technology/2023/apr/06/australian-mayor-prepares-worlds-first-defamation-lawsuit-over-chatgpt-content) : se está preparando para demandar por difamación.

No son solo las personas las que están preocupadas por cómo se utilizan los datos. Samsung ha prohibido a los empleados el uso de herramientas de inteligencia artificial generativa, en parte por temor a cómo se almacenan los datos en servidores externos y al riesgo de que los [secretos de la empresa puedan finalmente revelarse a otros usuarios](https://www.bloomberg.com/news/articles/2023-05-02/samsung-bans-chatgpt-and-other-generative-ai-use-by-staff-after-leak) . (Hay cuestiones separadas sobre  [los derechos de autor](https://www.lexology.com/pro/content/openai-fights-back-against-copyright-infringement-data-claims) y la propiedad intelectual).

En respuesta al escrutinio, particularmente del regulador de datos italiano, que ahora ha permitido que ChatGPT regrese al país  [después de que OpenAI hizo cambios en su servicio](https://www.gpdp.it/home/docweb/-/docweb-display/docweb/9881490#english) , la compañía introdujo herramientas y procesos que permiten a las personas tener más control sobre al menos algunos de sus datos. Aquí se explica cómo usarlos.

**Elimina tus datos de ChatGPT**

ChatGPT y  [GPT-4](https://www.wired.com/story/gpt-4-openai-will-make-chatgpt-smarter-but-wont-fix-its-flaws/) generan sus respuestas similares a las humanas estadísticamente, prediciendo qué palabras es probable que sigan a otras después de ver millones de ejemplos de oraciones escritas por autores humanos. OpenAI ha mantenido en secreto los datos con los que ha entrenado sus  [grandes modelos de lenguaje](https://www.wired.com/story/how-chatgpt-works-large-language-model/) , por lo que nadie fuera de la empresa sabe exactamente cuánto de la web (incluida la información personal de las personas) ha extraído en el proceso.

OpenAI dice que sus grandes modelos de lenguaje están entrenados en tres fuentes de información: datos tomados de la web, datos que la empresa otorga bajo licencia a otros y la información que la gente le da a través de chats. Esto puede incluir información sobre individuos. “Una gran cantidad de datos en Internet se relaciona con personas, por lo que nuestra información de capacitación incluye información personal”, explica OpenAI en una  [publicación](https://help.openai.com/en/articles/7842364-how-chatgpt-and-our-language-models-are-developed) , afirmando que toma medidas para reducir la cantidad que recopila.

OpenAI ahora ha introducido un [formulario de solicitud de eliminación de datos personales](https://share.hsforms.com/1UPy6xqxZSEqTrGDh4ywo_g4sk30) que permite a las personas, principalmente en Europa, aunque también en Japón, solicitar que se elimine su información de los sistemas de OpenAI. Se describe en una publicación de blog de OpenAI sobre cómo la empresa  [desarrolla sus modelos de lenguaje](https://help.openai.com/en/articles/7842364-how-chatgpt-and-our-language-models-are-developed) .

El  [formulario](https://share.hsforms.com/1UPy6xqxZSEqTrGDh4ywo_g4sk30) parece ser principalmente para solicitar que se elimine la información de las respuestas que ChatGPT brinda a los usuarios, en lugar de sus datos de capacitación. Le pide que proporcione su nombre; correo electrónico; el país en el que se encuentra; si está haciendo la solicitud para usted o en nombre de otra persona (por ejemplo, un abogado que hace una solicitud para un cliente); y si es una persona pública, como una celebridad.

OpenAI luego solicita evidencia de que sus sistemas lo han mencionado. Le pide que proporcione "indicaciones relevantes" que hayan resultado en su mención y también para cualquier captura de pantalla donde se le mencione. “Para poder atender adecuadamente sus solicitudes, necesitamos evidencia clara de que el modelo tiene conocimiento del sujeto de datos condicionado a las indicaciones”, dice el formulario. Le pide que jure que los datos son correctos y que comprende que OpenAI no puede, en todos los casos, eliminar los datos. La compañía dice que equilibrará "la privacidad y la libertad de expresión" al tomar decisiones sobre las solicitudes de eliminación de las personas.

Principio del formulario

Final del formulario

Daniel Leufer,  [analista principal de políticas](https://twitter.com/djleufer) de la organización sin fines de lucro de derechos digitales Access Now, dice que los cambios que OpenAI ha realizado en las últimas semanas están bien, pero que solo se trata de "la fruta madura" en lo que respecta a la protección de datos. “Todavía no han hecho nada para abordar el problema sistémico más complejo de cómo se usaron los datos de las personas para entrenar estos modelos, y espero que este no sea un problema que vaya a desaparecer, especialmente con la creación del grupo de trabajo EDPB  [sobre ChatGPT](https://edpb.europa.eu/news/news/2023/edpb-resolves-dispute-transfers-meta-and-creates-task-force-chat-gpt_en) ”, dice Leufer, refiriéndose a los reguladores europeos que se unen para analizar OpenAI.

“Las personas también pueden tener derecho a acceder, corregir, restringir, eliminar o transferir su información personal que puede estar incluida en nuestra información de capacitación”, también  [dice la página del centro de ayuda](https://help.openai.com/en/articles/7842364-how-chatgpt-and-our-language-models-are-developed) de OpenAI . Para ello, recomienda enviar un correo electrónico a su personal de protección de datos a dsar@openai.com. Las personas que ya solicitaron sus datos de OpenAI  [no quedaron impresionadas con sus respuestas](https://www.linkedin.com/posts/alexanderhanff_openai-cease-and-desist-letter-activity-7054088690901409792-2LXI/) . Y el regulador de datos de Italia dice que  [OpenAI afirma que es "técnicamente imposible"](https://www.gpdp.it/home/docweb/-/docweb-display/docweb/9881490" \l "english" \t "_blank) corregir imprecisiones en este momento.

**Cómo eliminar tu historial de chat de ChatGPT**

Debe tener cuidado con lo que le dice a ChatGPT, especialmente dadas las opciones limitadas de eliminación de datos de OpenAI. Las conversaciones que tiene con ChatGPT pueden, de forma predeterminada, ser utilizadas por OpenAI en sus futuros modelos de lenguaje grande como datos de entrenamiento. Esto significa que la información podría, al menos en teoría, reproducirse en respuesta a futuras preguntas de las personas. El 25 de abril, la compañía presentó una  [nueva configuración para permitir que cualquier persona detenga este proceso](https://openai.com/blog/new-ways-to-manage-your-data-in-chatgpt) , sin importar en qué parte del mundo se encuentre.

Cuando inicie sesión en ChatGPT, haga clic en su perfil de usuario en la esquina inferior izquierda de la pantalla, haga clic en **Configuración** y luego **en Controles de datos**. Aquí puede **desactivar Historial de chat y capacitación**. OpenAI  [dice que](https://help.openai.com/en/articles/7730893-data-controls-faq) desactivar su historial de chat significa que los datos que ingresa en las conversaciones "no se utilizarán para entrenar y mejorar nuestros modelos".

Como resultado, todo lo que ingrese en ChatGPT, como información sobre usted, su vida y su trabajo, no debería volver a aparecer en iteraciones futuras de los grandes modelos de lenguaje de OpenAI. OpenAI dice que cuando se desactiva el historial de chat, conservará todas las conversaciones durante 30 días "para controlar el abuso" y luego se eliminarán de forma permanente.

Cuando su historial de datos está desactivado, ChatGPT le indica que lo vuelva a activar colocando un botón en la barra lateral que le brinda la opción de habilitar el historial de chat nuevamente, un marcado contraste con la configuración "desactivada" enterrada en el menú de configuración.