

SAFETY · 10 min read · October 7, 2026 · By Kelly Stratton

Privacy Settings to Check Before You Try an AI Agent

Keep your messages, photos, and accounts yours while you try AI agents like Meta's Muse, ChatGPT, and Claude. You get the five Muse settings to check first, then the ones on Facebook and Instagram, on your iPhone and your Mac, and inside ChatGPT, Claude, and Google, with the exact taps for every one.

You're about to try one of the new AI agents, and you should. They can watch your inbox, keep your calendar straight, and do the errands you keep putting off. You just want to be the one deciding what they see. This guide gives you the exact settings to check in about fifteen minutes: inside Muse first, then on Facebook and Instagram, on your iPhone and your Mac, and inside ChatGPT, Claude, and Google. Each one has the taps, in order, and a plain reason for why it matters.

IN A NUTSHELL

An AI agent is an AI that does tasks for you instead of only answering questions. It can open websites, read your email or calendar if you connect them, and take actions on your behalf. The more it can see, the more it can do, so the permissions are the whole game.

WHAT YOU NEED

Your phone, your computer if you use an AI app on it, and about fifteen minutes. Nothing to install. Every step below is a setting you already have.

PART 1 What Happened With Meta's Muse?

Inc. columnist Jason Aten installed Meta's new AI agent, Muse, on his iPhone and a Mac to try it. He says he chose not to give it access to his messages, calendar, or other personal information. Soon after, he was texting with a friend, his podcast co-host, about the new iPhones when Muse sent him a notification suggesting that conversation would make a good story. When he asked how it knew, Muse told him it was only seeing the text of incoming notification banners. He says he then found that Muse had synced his Mac's Messages database, through row 187,462, while Full Disk Access on his Mac showed as off.

Meta disputes his account. Meta's Andy Stone, its head of communications, said the Messages feature in the Muse app for Mac is entirely opt-in: "You have to enable both Full Disk Access and the Messages connector for Muse to be able to read your Messages content. It can't read your Messages unless you do this." Meta's David Singleton said reading Messages takes three separate permission steps and that the Mac's own protections can't be circumvented, even by a bug. Aten says Full Disk Access was off on his Mac, and as of this writing the two sides still disagree.

You don't have to settle that argument to act on it. The lesson is the same either way: before you hand an agent your accounts, know exactly what you've allowed, and check it yourself instead of trusting the setup screen. Meta already has a lot of your information if you use Facebook or Instagram, and Muse connects to those automatically when the accounts share an Accounts Center. The rest of this guide is the checking.

PART 2 Which Muse Settings Should You Check?

If you've installed Muse, do these five first. They're the settings behind the story, and they take about five minutes. The first, second, and fifth are inside the Muse app on any device. The third and fourth are for the Mac app.

1. See what Muse is connected to.

1. Open **Settings**, then **Connectors**.
2. Expect Facebook, Instagram, and Threads on the list. Meta connects them on their own when those accounts are in the same Accounts Center as Muse.
3. Tap **Disconnect** on anything you didn't mean to connect, like your email or your calendar.

Disconnecting stops Muse from exchanging data with that service. What it already pulled in can stay in your chats and its memory. Part 8 covers clearing that.

2. Make Muse ask before it acts.

1. Open **Settings**, then **Permissions**.
2. You'll see two settings, **Connectors** and **Web access defaults**. Each one offers **Ask for some actions** or **Always ask**.
3. Choose **Always ask** for both. In Meta's words, Muse will then ask before any action in a connected app and before accessing any website. "Ask for some actions" is looser: for Connectors it asks before every write and important read, and for websites it asks only when your information may be shared or the site is unfamiliar.
4. Below those, **Manage permissions** lets you set each Connector on its own, approve each scheduled task, and open **Allowed websites**, where you can revoke any site you've let Muse into.

3. On a Mac, set what Muse can read, app by app.

1. In the Muse app on your Mac, open **Settings**, then **File System Access**.
2. Every app that keeps information on your Mac is listed: Messages, Mail, Notes, Calendar, and others. Each one is set to **Off**, **Read only**, or **Read and interact**.
3. Set anything you didn't choose yourself to **Off**. In Meta's words, Off means "your agent can't use the information that app keeps on your Mac." Messages is the one from the story. Meta's statement calls that setting "the Messages connector"; on Meta's help page, this per-app switch is where it lives.

4. Check your Mac's own permissions for Muse.

1. Open **System Settings** from the Apple menu, then **Privacy & Security**.
2. Meta's help page names three permissions Muse asks for: **Full Disk Access**, **Automation**, and **Notifications**. Open each list and find Muse.
3. Switch Muse off in **Full Disk Access** unless you want it able to read files anywhere on your Mac, including the data behind Messages and Mail. This is the other half of Meta's statement: without it, Meta says Muse can't read your Messages.
4. Switch Muse off in **Automation** if you only want it to read your apps, not act inside them. Notifications can stay on. It only lets Muse tell you when a task is done.

5. Decide whether your chats train Meta's AI.

1. Open **Settings**, then **Data controls**.
2. The switch that lets your Muse interactions train Meta's AI is on by default, in Meta's words. Turn it off if you'd rather not.
3. The same page has **Download your Muse data**, and **Reset Muse**, which deletes your chat history, files, and active tasks and can't be undone.

When those five are done, you know what Muse is connected to, it asks before it acts, nothing on your Mac is readable unless you set it, and your chats train the model only if you choose. Now the rest of your accounts.

PART 3 Which Facebook and Instagram Settings Should You Check?

Start here, because this is where most people have years of forgotten connections. Every quiz, game, and “log in with Facebook” button you ever tapped may still be on the list.

1. Remove apps and websites you don’t use from Facebook.

1. On a computer, click your profile picture in the top right, then **Settings & privacy**, then **Settings**.
2. Click **Apps and websites** in the left menu. In the Facebook app, the same page is under **Settings & privacy**, then **Settings**. Look for **Apps and websites**.
3. Open the **Active** tab. This is every app and site that can currently see your Facebook information.
4. Click **Remove** next to anything you don’t recognize or don’t use, then **Remove** again to confirm.

Removing an app stops it from seeing your non-public information from now on. It may still have what it collected before, and you can contact the developer and ask them to delete it.

2. Do the same on Instagram.

1. In the Instagram app, open your profile and tap the three lines in the top right. The screen that opens is **Settings and activity**.
2. Scroll to **App website permissions** and tap **Apps and websites**.
3. You’ll see three tabs: **Active**, **Expired**, and **Removed**. Open **Active** and tap **Remove** next to anything you don’t use.

On a computer, click **More** in the bottom left, then **Settings**, then **Website permissions** under **Your app and media**, then **Apps and websites**.

If your account is private and you haven't logged into an app with Instagram in the last 90 days, its access to your non-public information expires on its own. Removing it now saves you the wait.

3. See what Meta collects from other apps and websites.

In either app, open **Settings**, then **Accounts Center**, then **Your information and permissions**, then **Your activity off Meta technologies**. This is the record of what other businesses send Meta about you, like a visit to their website or a purchase in their store. Use **Clear history** to disconnect what's there, and **Manage future activity** to stop new activity from being connected. It's also the one page that shows you, in plain words, how much Meta already knows.

4. Know where the AI controls live.

Meta's page on how it uses your information for AI is at facebook.com/privacy/guide/genai. It explains what Meta uses, including public posts and your chats with its AI, and it links to the forms for seeing and deleting that information. Muse's own switch for this is in Part 2, step 5.

PART 4 Which Permissions Should You Check on Your Phone and Computer?

Your phone and your computer keep their own permission lists, separate from any account. This is the list that mattered in the Muse story, so look at it before you install an agent and again after.

On your iPhone

1. Open **Settings**, then **Privacy & Security**.
2. Tap each category you care about: **Contacts**, **Calendars**, **Photos**, **Microphone**, **Camera**, and **Location Services**. Each one lists the apps that asked for it.

3. Find any AI app on the list and switch it off, or set Photos to **Limited Access** so it sees only the pictures you pick.
4. Scroll to the bottom of Privacy & Security, tap **App Privacy Report**, and tap **Turn On App Privacy Report**. From now on, it shows you which apps used your location, camera, microphone, contacts, and more, and how often, over the past seven days. Check it a week after you try any new agent.

On your Mac

Open **System Settings** from the Apple menu, click **Privacy & Security** in the sidebar, and look at these four lists. Each one shows the apps that have the permission, with a switch beside each app.

The four Mac permissions to check

Full Disk Access

Lets an app read every file on your Mac, including the data behind Messages, Mail, and Safari. This is the permission in the Muse story. Only give it to an app that truly needs it, and switch it off for any AI app you're just trying out.

Automation

Lets an app control other apps, like reading or sending in Mail or Messages. Muse asks for this so it can act inside your apps. Switch it off if you only want the agent to read.

Files & Folders

Lets an app into your Desktop, Documents, and Downloads folders. A narrower choice than Full Disk Access for an agent that only needs your files.

Accessibility and Screen & System Audio Recording

Let an app see your screen and click for you. An agent that clicks and types on your Mac for you asks for these. Turn them off when you're not using the agent for that.

A permission can come back on after an app updates or asks again, so this is a list to look at every month, not once.

PART 5 What Should You Check Inside the AI Tools Themselves?

Muse isn't the only agent with its own switches. ChatGPT, Claude, and your Google Account each keep a list of what's connected, and each one has a Disconnect button.

Where the switches are in ChatGPT, Claude, and Google

ChatGPT

Open Settings, then Apps. Pick an app, and if you see Connected accounts, open the three-dot menu next to the account and choose Disconnect. OpenAI says disconnecting stops future access through that account. For an app that synced your files, like Google Drive, the synced copy is deleted within 30 days.

Claude

Open Customize, then Connectors. Click any connected service to see its permissions, and click Disconnect to remove it. The toggles under the plus button in a chat only turn a connector off for that one conversation; the Customize page is where you remove it for good.

Your Google Account

Go to myaccount.google.com/connections. Under Have access to your Google Account, you'll see every tool that can read your Gmail, Calendar, or Drive, including any AI agent you connected. Open one and click Remove access, then Confirm. This cuts the access from Google's side, whatever the tool's own settings say.

PART 6 How to Decide What to Connect

You don't have to say no to everything. You have to say yes on purpose. Four rules keep you in charge.

Connect only what the job needs. An agent watching a flight price needs a web browser, not your email. An agent writing your morning brief needs your calendar, not your photos. When a setup screen asks for everything, skip it, and add a connection

later when a specific job calls for it.

Start with read-only. Reading your calendar is one thing. Sending, deleting, and buying are another. Where a tool offers a read-only choice, like Muse's **Read only** per app, take it first.

Keep "ask before acting" on. Muse has it under Permissions (Part 2, step 2), and a ChatGPT Dot has it under Custom rules in Settings. It makes the agent check with you before it sends, buys, or changes something. Leave it on until you've watched the agent work for a while.

Check again after every update. Settings move and permissions get re-asked. The App Privacy Report on your iPhone and the Privacy & Security lists on your Mac are a two-minute look once a month.

PART 7 The Tell

Here's how you'd know an agent has more access than you gave it.

What you're seeing, and what to do

It brings up something you never told it

A message, a plan, a name from a conversation it shouldn't have seen. That's the exact sign from the Muse story. Go back through Parts 2 to 5 and look at every list before you type another word to it.

A permission you turned off is back on

Apps can ask again after an update. Switch it off again, and consider removing the app from Full Disk Access entirely.

A name you don't recognize in Apps and websites

Remove it. If it posted anything on your behalf, Facebook will ask whether to delete those posts too. Say yes.

Your App Privacy Report shows an app using your microphone or location when you weren't using the app

Turn that permission off for the app, and decide whether you need the app at all.

PART 8 Where You Still Come In

Turning access off doesn't delete what was already copied. It stops new reading. In Muse, **Settings**, then **Data controls**, then **Reset Muse** clears everything, and it can't be undone. Meta also says you can ask Muse in the chat to forget one specific thing. In other tools, delete the chats and memories, and ask the company to delete your data if you want to be sure.

The setup screen is not the check. What you clicked during setup is a request. The permission lists on your phone and computer are the truth. Look at those.

Trust the agent after it earns it. Give it one small job with one connection, watch what it does for a week, and then widen it. You get the help, and your information stays yours.

DO THIS FIRST

If you have Muse, open Settings, then Permissions, and set both switches to Always ask. Then open Facebook's Apps and websites page and remove everything you don't recognize. Those two take five minutes, and they're the ones most people have never looked at.

Straight answers

What is an AI agent?

An AI agent is an AI that does tasks for you instead of only answering questions. It can open websites, read your email or calendar if you connect them, and take actions like drafting a message or filling a cart. Meta's Muse, ChatGPT's Dots, and Claude with connectors are all AI agents.

Did Meta's Muse really read someone's private messages?

Inc. columnist Jason Aten says it did. He reports that Muse suggested a story based on his texts after he declined to give it access to Messages, and that it had synced his Mac's Messages database while Full Disk Access was off. Meta disputes this and says the Messages feature is opt-in and can't read your Messages unless you turn on two settings yourself.

What is Full Disk Access on a Mac?

It's a Mac permission that lets one app read every file on your computer, including the data behind Messages, Mail, and Safari. You'll find it in System Settings under Privacy & Security. Give it only to apps that truly need it, and check the list after you install any AI app.

How do I see which apps are connected to my Facebook or Instagram?

On Facebook, open Settings & privacy, then Settings, then Apps and websites. On Instagram, open your profile, tap the three lines, then App website permissions, then Apps and websites. Each one shows an Active list with a Remove button next to every app that can see your account.

How do I stop an AI agent from reading my email or calendar?

Disconnect it inside the tool. In Muse, open Settings, then Connectors. In ChatGPT, open Settings, then Apps. In Claude, open Customize, then Connectors. You can also remove the tool from your Google Account at myaccount.google.com/connections, which cuts the access from Google's side.

Does turning a permission off delete what the agent already copied?

No. Turning access off stops new reading. Anything already pulled in can stay in the tool's chat history or memory. In Muse, Settings, then Data controls, then Reset Muse clears it. In other tools, delete the chats and memories, and ask the company to delete your data if you want to be sure.

Should I stop using AI agents altogether?

No. The fix is control, not avoidance. Connect only what a job needs, start with read-only access, keep the setting that makes the agent ask before it acts, and look at your permission lists once a month and after every update. You get the help and keep your information yours.

SOURCES Where This Comes From

- [Inc., Jason Aten: Meta's New Muse AI Agent Read My Private Messages. I Never Asked It To](#), for what he says happened.
- [TechCrunch: Meta disputes claim that Muse read a user's private messages without permission](#), for Meta's response and the quotes from Andy Stone and David Singleton.
- [Meta: How Muse works with files and apps on your Mac](#), for Full Disk Access, Automation, and the File System Access settings.
- [Meta: How Muse works with Connectors](#) and [How Muse handles your privacy, safety and security](#), for Connectors, Permissions, and Data controls.
- [Meta: How to manage your Muse data](#), for Reset Muse.
- [Facebook Help: Remove an app or game that you've added to Facebook](#) and [Instagram Help: Manage the privacy settings for apps and websites](#), for the Apps and websites steps.
- [Apple: Controlling app access to files in macOS](#) and [Apple: About App Privacy Report](#), for the Mac and iPhone permissions.

- [OpenAI: Connecting and managing app accounts in ChatGPT](#), [Anthropic: Use connectors to extend Claude's capabilities](#), and [Google: Manage connections between your Google Account and third parties](#), for the disconnect steps.

Want *more* like this?

Free AI guides added regularly. No jargon, no overwhelm.

[**kellystrattonai.com**](https://kellystrattonai.com)

Instagram / TikTok: @kellystratton.ai | Facebook / YouTube: @kellystrattonai