How to turn off Windows Telemetry to protect privacy

Telemetry is, in theory, how Microsoft collects information from users' computers. According to the company, this helps identify bugs, improve performance, and deliver updates that are tailored to the way people use Windows.

People spend a lot of time tinkering with Windows settings to make their computers run faster, more smoothly, or simply less annoying. But there's a hidden setting that does the opposite of protecting us. It doesn't speed up or keep your system running smoothly. Instead, it silently sends information out of your computer without you even knowing.

What is Windows Telemetry?

Microsoft says it has improved updates, but the reality is different.

In theory, telemetry is how Microsoft collects information from users' computers. According to the company, this helps identify bugs, improve performance, and deliver updates that are tailored to the way people use Windows. The idea is that by studying millions of systems, Microsoft can identify problems faster and deliver fixes more effectively.

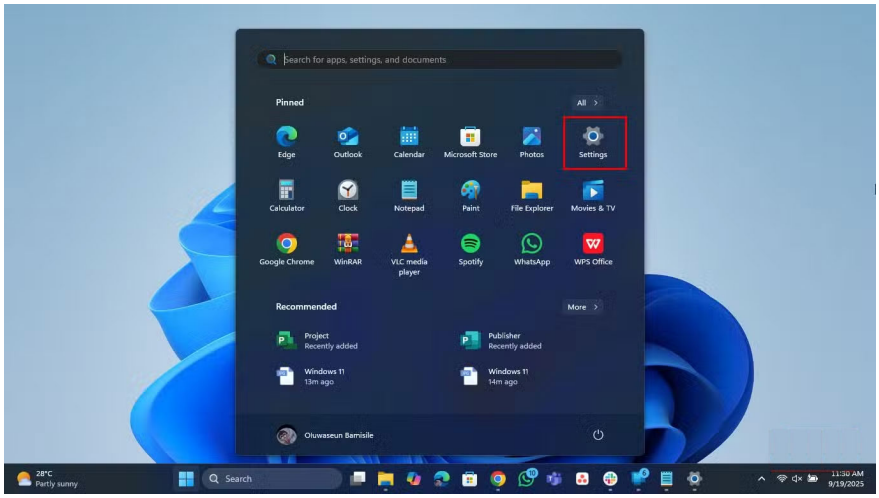
That's the official marketing message. In reality, it goes beyond bug reporting. Telemetry collects detailed information about your system configuration, the apps you install, how often you use them, the type of hardware

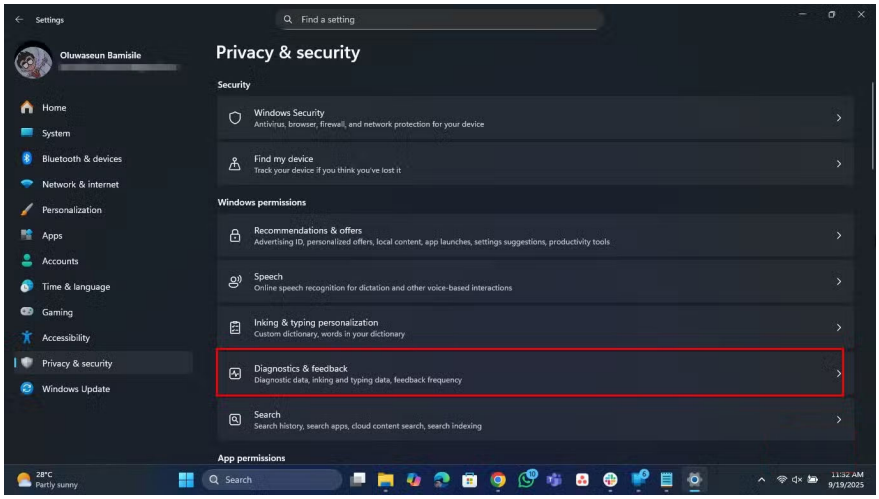
you run, and even your daily activities. Microsoft assures us that the data is anonymized, but if you've ever dealt with so-called anonymized datasets, you know that's not always as trustworthy as you think.

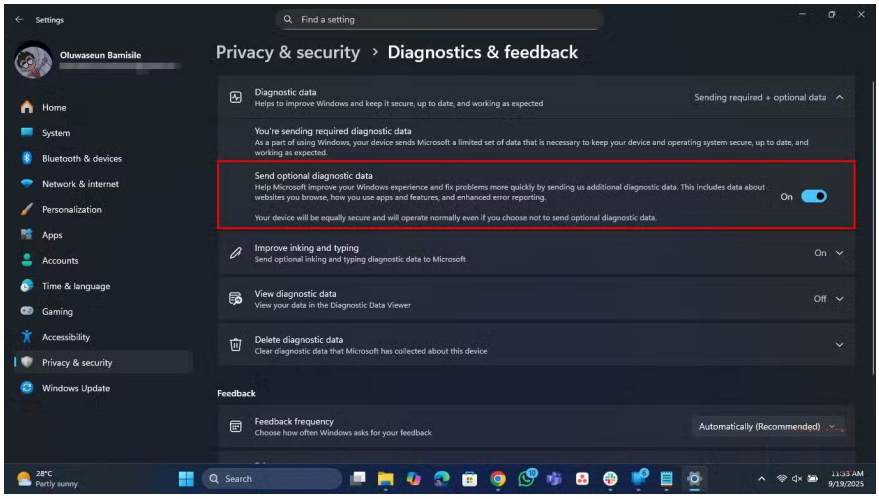
When the Telemetry vulnerability was first discovered, many people were a bit surprised. They had always assumed that crash reporting was voluntary, something you submitted when a program crashed. Instead, Telemetry was built-in, turned on by default, and designed to run continuously in the background.

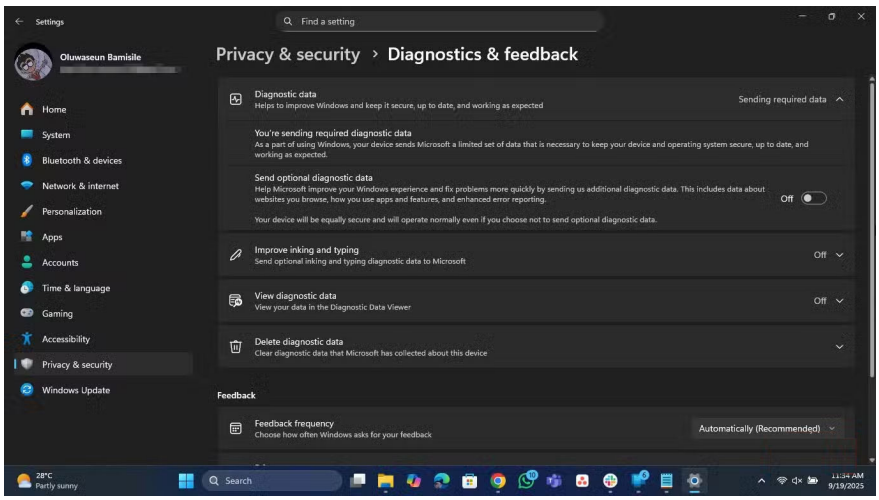
How to Turn Off Telemetry in Windows

You can't completely remove it, but you can minimize it.









You can turn off most Telemetry data collection features, even if Microsoft doesn't explicitly state it.

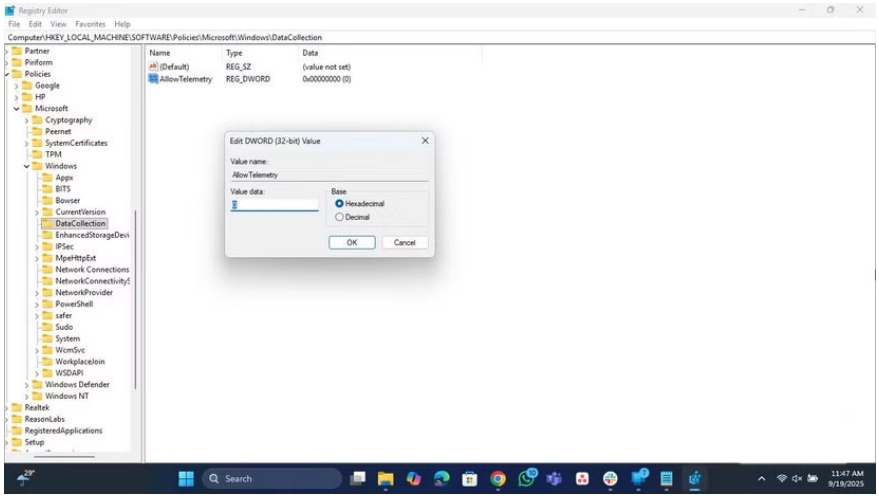
1. Open the Settings app
2. Go to **Privacy & Security**
3. Select **Diagnostics & feedback**
4. Under **Diagnostic data , turn off the Send optional diagnostic data** option.

That's step one, and it's already significantly reduced tracking. But if you're running Windows Pro, Enterprise, or Education, you can take it further using the Group Policy Editor.

How to do it:

1. Press **Win + R** , type **"gpedit.msc"** and press **Enter** .
2. Navigate to **Computer Configuration -> Administrative Templates -> Windows Components -> Data Collection and Preview Builds** .
3. Double-click **Allow Diagnostic Data** (Windows 11) or **Allow Telemetry** (Windows 10) and set it to **Disabled** .

If you are familiar with Registry Editor, you can do the same thing by opening Registry Editor and adding a DWORD key named **AllowTelemetry** to **HKEY_LOCAL_MACHINESOFTWAREPoliciesMicrosoftWindowsDataCollection** and setting its value to **0** .



After doing this, your system will stop communicating back to the center for Telemetry data. Updates will still occur, but the constant background reporting noise will be significantly reduced. You should notice a difference almost immediately after disabling it - fewer random spikes in network usage and a smoother, quieter system.

Control your data

If you care about privacy in the slightest, turning off telemetry is non-negotiable. It may seem harsh, but you should still stand firm. Microsoft should be transparent and give users a clear 'off' button, but since it won't, we have to take control. No one wants to live in a world where every click and keystroke is silently recorded just to 'improve the user experience.' You deserve better. Your computer should serve you, not Microsoft.