RECLAIM THE NET [(https://reclaimthenet.org)](https://reclaimthenet.org)

# WiFi is exposing your location to Big Tech and data brokers. Here's how to protect yourself.

**Share ()**

When you use the internet, there are many ways you can be tracked. But even when you're not connected to the internet, your device's WiFi connection features can still be used to track your movements and potentially expose other data about you to third parties.

This data is exposed via "probe requests" — a type of request your device and other nearby

WiFi-enabled devices use to find and connect to WiFi networks.

There are two types of probe requests — passive requests and active requests.

Passive requests look for WiFi networks that your device has previously connected to and allow your device to automatically connect to these networks.

Your device can make these automatic connections because it automatically saves the name of every WiFi network your device has previously connected to a “preferred network list.” It then constantly listens for “beacons” (constant announcements that are sent out by WiFi networks and contain information allowing devices to identify them). If your device recognizes a nearby WiFi network that’s on your preferred network list, it will automatically connect to this network.

The only way to prevent WiFi networks from being added to this preferred network list is to manually forget each network after connecting to it for the first time.

With active requests, your device actively sends out requests to nearby WiFi devices asking if they’re a WiFi network. Nearby WiFi networks then respond to these requests and identify themselves to your device.

## How probe requests can leak your data

Both types of probe requests can leak information that can be used to track and identify your device and even expose the entire list of WiFi networks that you’ve previously connected to.

Here is some of the data that can be leaked to third parties via probe requests:

### 1. Your preferred network list

One of the most sensitive pieces of information that can be leaked via some of these probe requests is your preferred network list. This exposes the entire list of WiFi networks that you’ve previously connected to.

The names of the WiFi networks that you connect to can be very revealing. For example, names such as “Best Quality New York Repair Shop Staff WiFi,” “Privacy Conference 2022 WiFi,” “Bob Jones’ WiFi,” and “Xfinity Home WiFi” would reveal a person’s interests, the place they work, the name of one of their contacts, and their home WiFi provider. Some WiFi network names even contain the full address of where the network is located.

Not only does exposing your full preferred network list to third parties give them access to revealing information but it also serves as a unique identifier that can be used by third parties to track you. Very few people, if any, are going to have the same preferred network list as you. This uniqueness allows third parties to associate these preferred network lists with you and your devices.

Most modern devices and operating systems partially address this issue by sending out a wildcard instead of the preferred network list when making probe requests to public networks. However, even modern devices and operating systems still send out a preferred list of hidden networks when connecting to hidden networks.

And even with the additional privacy protection offered by modern devices and operating systems, a recent study (https://deepai.org/publication/probing-for-passwords-privacy-implications-of-ssids-in-probe-requests) that collected and analyzed 252,242 probe requests in a busy area found that 23.2% of the probe requests were broadcasting the names of WiFi networks that the associated device had previously connected to. This study also found that some WiFi probe requests were broadcasting email addresses and passwords which the study’s authors presumed had been entered into the WiFi network name field by accident.

## 2. Identifiers

Some probe requests contain a device’s media access control (MAC) address (a unique device identifier) and sequence numbers (unique numbers that are assigned to sessions when devices attempt to connect to the internet). Third parties can use MAC addresses to track your devices and sequence numbers to get some information on your internet sessions.

While modern devices and operating systems make these identifiers more private by randomizing them and preventing third parties from being able to see your real MAC addresses or sequence numbers, some researchers (https://deepai.org/publication/probing-for-passwords-privacy-implications-of-ssids-in-probe-requests) have managed to associate probe requests from randomized MAC addresses and concluded that MAC address randomization is insufficient to prevent tracking.

## How these probe requests impact your privacy and security

Not only do probe requests have the potential to leak your sensitive data but they can also create many privacy and security issues.

Data profiling companies can track the times and locations of probe requests and then use the preferred network list to tie probe requests from the same device together. Once they've tied these probe requests together, these companies can track the times and locations of the probe request to map the movements of devices.

Data profiling companies can also combine the revealing information that they've gathered from a unique preferred network list with information from other data brokers to build a detailed profile on individual devices and their users.

Hackers and other bad actors can collect the same data as these data profiling companies and use it for malicious purposes. If your device leaks this information via probe requests, hackers or bad actors could see whether you're at home, see if you're alone, or use it to build a more detailed profile for the basis of a social engineering attack.

Hackers can also set up a malicious network that pretends to be a well-known public WiFi network and trick devices into automatically connecting to them via passive probe requests. Once a device has been tricked into connecting to a malicious network in this way, a hacker could perform man-in-the-middle attacks and monitor unencrypted internet activity.

## Protecting yourself from probe request data leaks

Although probe requests are a potential privacy and security nightmare, there are things you can do to protect yourself.

Here are some steps you can take to stop your data from being leaked via probe requests:

## 1. Turn off WiFi when you’re not using it

The easiest way to stop your data from being leaked via probe requests is to turn off WiFi when you’re not using it. When WiFi is off, your device won’t make any probe requests.

Note that on Android you’ll need to turn off WiFi (which can be accessed by opening the “Settings” app and selecting “Connections”) and “Nearby Device Scanning” (which can be accessed by opening the “Settings” app and selecting “Connections” > “More Connection settings”).

On Apple (https://reclaimthenet.org/topics/apple/) devices, you can’t just turn off WiFi via Control Center. Instead, you need to turn open the “Settings” or “System Preferences” app, select “Wi-Fi,” and disable WiFi from this menu.

You can automatically disable WiFi with Shortcuts on Apple devices (https://www.iphonelife.com/content/how-to-set-iphone-wi-fi-to-automatically-turn-when-you-leave-home) using time-based conditions (e.g. automatically disable WiFi every day at 9 am), location-based conditions (e.g. automatically disable WiFi when you leave home), and conditions based on other parameters. However, some of these automations will require you to enable location data sharing on your devices.

## 2. Remove WiFi networks from your preferred network list

By removing most or all of the WiFi networks from your preferred networks list, you can limit the amount of data that’s exposed when your phone makes probe requests.

Macs and most non-Apple devices let you see your preferred network list and remove networks from this list in the WiFi settings. However, other Apple devices don’t let you see your preferred network list which leaves you with two options if you use these devices.

The first option is to forget WiFi networks as you come back into contact with them by opening the Apple devices' WiFi settings, tapping the network, and selecting "Forget This Network."

This option ensures that you don't inadvertently remove networks that you want to use. However, WiFi networks that you never reconnect to, such as networks you used while traveling or on vacation, will remain on your preferred network list.

The second option is to remove all of the WiFi networks from your device by opening the Apple devices' settings and selecting "General" > "Transfer or Reset [Device Type]" > "Reset" > "Reset Network Settings."

This option clears all of the saved WiFi networks, cellular settings, virtual private network (VPN) settings, and access point name (APN) settings from your device and ensures that all unwanted networks are cleared from your device. However, since it also removes WiFi networks that you want to use, you'll have to manually reconnect to these networks after resetting your network settings. Additionally, you may have to reconfigure your cellular settings and VPN settings after performing the reset.

## 3. Disable auto-join for WiFi networks

If there are some WiFi networks that you want to keep on your preferred network list but don't need to automatically connect to, disable auto-join for these networks. Most devices let you toggle auto-join for each of the networks listed in your WiFi settings.

After you've disabled auto-join for the existing networks on your list, consider whether you need to automatically connect to each new WiFi network that you connect to in the future. If you don't need an automatic connection, disable auto-join before making the first connection to the network. You can usually toggle auto-join for new networks in your WiFi settings when making the connection for the first time.

By disabling auto-join, you may limit the information that's broadcast during probe requests.

### 4. Choose a less revealing name for your home WiFi network

Your home WiFi network's name may contain revealing details such as your name, your internet service provider (ISP), your router brand, or your router model number. Any information in your home WiFi network's name could be leaked via probe requests from your phone and any other phones that connect to your home network.

By changing the network name to something less revealing, such as a random word or phrase, you can prevent sensitive information from being exposed via your home WiFi network name.

The option to change your router name will usually be under an "Advanced" or "Wireless" section of your router's settings.

### 5. Keep your device operating systems up to date

Most of the features that boost your WiFi privacy are only available in modern operating systems. Additionally, any future WiFi privacy features are likely to be released in the latest operating systems.

Therefore, you should keep your devices up to date with the latest operating systems to ensure that you have access to all of the built-in WiFi privacy features that are available. On most devices, you can automate the process of keeping the operating systems up to date by enabling the automatic updates feature.

## Level up your WiFi privacy and security

After implementing these tips, make sure you read up on these other WiFi privacy issues (https://reclaimthenet.org/wifi-signals-can-be-incredibly-privacy-invasive/) and change these router settings (https://reclaimthenet.org/make-these-changes-to-your-router-to-patch-security-holes-and-increase-internet-speed/) to further boost your WiFi security and speed.

And be sure to share these tips with anyone else who would benefit from leveling up their WiFi privacy and security.