

Forum:[Hack Forums](#)

Thread: [Why do some websites still detect your real country?](#)

1stShepherd - March 30, 2026, 6:40 pm

You turn on your VPN and your IP changes. It feels like you should be invisible, but some websites still know exactly where you are.

Your IP is just one clue. Websites also look at your browser's timezone (for example, "Asia/Kolkata" doesn't match a German IP), your Accept-Language header (en-IN gives you away), and your DNS resolver, which is probably still set to your ISP's servers back home instead of your VPN's.

One of the sneakiest trick is WebRTC. Your browser has a built-in feature for video calls that can fetch your real IP address at the operating system level, completely bypassing the VPN tunnel. A website can get it with just 10 lines of JavaScript. Some VPNs don't block this by default.

And if you're logged in, it's game over. Netflix, Google and Spotify don't care about your IP address. They care about your account. Your registered country is stored in their database, not in your connection. Using a VPN while logged in means the VPN isn't helping you at all.

A VPN gives you a different postal address, but your timezone, language, DNS, WebRTC, browser fingerprint, and login details are still the same

XtremeDiscount - March 31, 2026, 9:00 am

Cookie data. Use icgonito mode + the vpn.

KnownSyntax - March 31, 2026, 9:17 pm

As the user above notes, this can be tied to cookie data (i.e. data already stored in your session before you switched to the VPN), but is more commonly due to your browser leaking your actual geofence location data (locale codes, sometimes country code, etc.). This is how they can see you are actually from Asia/Kolkata but yet your IP shows an ISP in German, which would flag you using a VPN or some other aspect that doesn't match.