When is “the cloud” not a cloud?

All the time. What we think of as a wireless, wispy cloud is in fact made up of a vast network of wires, servers, hubs, and buildings. When you access your email or Dropbox or other cloud-based services, your computer is sending a request for files from another physical computer that lives somewhere else in the world.

Here are a few tools that let you peek behind the curtain and give you an idea of how the internet really works.

How does a website get to your computer?

Pick a website and copy its URL. We’ll use nytimes.com here as an example.

On a Mac: Open Terminal (search for the program) and type `traceroute nytimes.com`

On a PC: Open Command Prompt (Start menu » All programs » Accessories) and type `tracert nytimes.com`

Browser option: Go to tools.pingdom.com/ping and choose traceroute (it’ll be testing from Pingdom’s computers, though, not yours). Type in the URL and submit.

`Traceroute` will show you all the routers (internet connector points) your computer must contact to request to access a webpage. It’s tracing a map across the city, or even the country, or even the world as your request travels from router to router to find the server (special computer) that hosts the website (stores the website’s files). Each router or server will display an IP address, the numerical address that only that machine is assigned.

So “nytimes.com” is actually just a human-readable version of the real web address for the New York Times, which is 170.149.172.130, a computer that is probably downtown. In between your computer and nytimes.com, there are many other IP addresses. Using some internet sleuthing skills, you can find out where these IP addresses are located geographically and/or who owns them.

**When to use this:** Use traceroute when you want to visualize how far away a website is, or when you want to diagnose whether a website is not loading because of a problem with your network, the website itself, or somewhere in between.

**Further reading:**
Bundled, Buried & Behind Closed Doors: video tour of network hubs and discussion from experts vimeo.com/30642376
Seeing Networks (NYC edition): a visual guide to the physical network in New York City seeingnetworks.in/nyc

Who owns this website?

Pick a website whose owner you want to know. We’ll use nissan.com as an example.

On a Mac or PC: From Terminal or Command Prompt, respectively, type `whois nissan.com`

Browser option: Go to http://who.is and type in the URL

`Whois` will show you who registered the website — the person and/or their organization. It will even give you their mailing address, email address, and phone number. (Not all websites will give you this personal information, but someone must be the registrant.) In this case, we can see that nissan.com, which looked funny in the browser from the start, is not owned by the Nissan car company, but by a man named Uzi Nissan in North Carolina who’s holding onto this URL despite a lawsuit.

**When to use this:** Use whois when a website looks fishy or seems like it might not be owned by who they say they are.
### Why do you and I see different search results?

When I search Google for “gun control,” my search results will be different from when you search for “gun control.” This happens for two reasons:

**PageRank**: Google’s super-secret, super-smart algorithm for determining which results are relevant and how to order them for a user. PageRank makes both of these decisions based on current events (gun control news), location of computer (different results for New York City vs. Dallas), and many other factors.

**Private results**: If you’re signed into Google, it will display many results it thinks you most want to see ranked higher than results that may not interest you, based on your past history of site visits and link clicks. A gun control advocate will see different results than a member of the NRA. Thanks to work from people who want to prevent a “filter bubble” (being shown only what you want to see), the difference may be negligible on the first page — but search results are never neutral, especially when you’re signed in. You can toggle between private results and “global” results (using location, etc.).

**When to use this**: When you’re curious about how a topic displays differently for different people. Try comparing the first three pages of results for a given search with a friend. Try keywords related to current events, shopping items, and controversial concepts.

**Further watching**: Beware Online ‘Filter Bubbles’: a 2011 talk from Eli Pariser about the non-neutrality of search results [ted.com/talks/eli_pariser_beware_online_filter_bubbles](http://ted.com/talks/eli_pariser_beware_online_filter_bubbles)

### Who does Google think you are?

Interested in seeing more about why your private results are what they are? You can go to [google.com/settings/ads](http://google.com/settings/ads) to see the list of information Google thinks it knows about you. Some data you’ve given Google outright in your Google+ profile; others it guesses. It can be hilarious and disturbing to look at what Google thinks are your “interests.” Using all of this data, plus more data you can’t see, Google decides which ads to display for you.

**When to use this**: Just once or twice is useful to see how Google envisions you as a list of semi-accurate information.

### Who’s tracking you?

**Cookies** are the delicious-sounding term for bits of invisible code that follow you as you browse the internet. Sometimes cookies are very useful, like when you’re shopping online and the website shows you things you looked at before. But sometimes cookies are more malevolent — they track you so that advertisers can target ads at you, or more maliciously, so private information about you can be gleaned for other purposes, like changing item prices based on how wealthy the website thinks you might be.

You can see what and who is tracking you using a number of browser plugins or add-ons. I recommend Ghostery ([ghostery.com](http://ghostery.com)) for Chrome, Firefox, Safari, and Internet Explorer. It will count how many trackers it detects on a website, who makes them, and what they’re used for. Ghostery will let you block specific trackers from all websites.

**When to use this**: All the time! It will change the way you view the websites you visit. Some pages will have only a few trackers for “analytics” (counting visitors); some will have dozens or even hundreds of “advertising beacons.”

---

Comparing “free speech terrorism” search results between a 26-year-old liberal woman’s account and a 50-year-old conservative man’s account
How do you remain anonymous?

At this point, having a hint of how other people and companies might use personal data that can be obtained when you’re just visiting webpages, you may wish to remain anonymous. But it’s almost impossible to be a truly “anonymous” browser without taking a ridiculous number of precautions. Even when you’re logged out of everything, your browser records your viewing history and caches cookies. Even when you clear your history and cookies, websites and trackers can still tell some things about you, like whether you use a Mac or PC, which neighborhood you’re in, and which internet provider you use.

One way to browse semi-anonymously without having to clear your history, clear cookies, or log out of anything is by opening a Private or Incognito window in your browser. The browser will not record which websites you look at, nor will it use any cookies or info it saved from previous web browsing.

**When to use this:** People often use a private browsing window when they are looking up a health issue, are researching a highly controversial issue they don’t want associated with their real identity, or just want to log into two email addresses at once.

**Further reading:** For true anonymity and security, you’ll need to do a deeper dive into keeping your information safe. Research keywords: HTTPS, encrypt, Tor, VPN.

Have you been hacked?

This is a question that is surprisingly hard to answer. Hacking may not always be apparent. But we still can still see some indications.

Weekly, we hear of a data breach or website hack at a big company. This happens for healthcare corporations, technology giants, retail companies, and banks alike — all organizations that take security precautions but which inevitably are hacked somehow. Hackers will sell long lists of users’ information on the black market for other hackers to use. Companies will also make some information publicly available. To see if your email address(es) or username(s) are included in a big-time hack, check haveibeenpwned.com (Have I Been Pwned).

**When to use this:** Check Have I Been Pwned semi-regularly. It’s fairly reliable for large-scale attacks. But keep your ears open for news of data breaches and major hacks, too. Sometimes companies whose servers have been attacked will notify the public, and sometimes they won’t.

**Further action:** Smaller instances of hacking, where someone targets you personally, may be harder to ascertain. Reset your important passwords at least once a year. Use passwords that are hard to guess. Monitor your important accounts for suspicious activity. Password-protect your wifi network at home. Use your home router’s dashboard to see a list of connected devices every now and then, to make sure you know who’s on your network.