# Who's Watching You Online?

*A Plain-English Guide to Digital Privacy*

Written for people who didn't grow up with the internet — but now live with it every day.

---

## You're being watched. Yes, really.

Every time you open a website, check your email, search for something on Google, or scroll through Facebook, you leave a trail. That trail is being collected, analysed, and used — by companies who want to sell you things, and increasingly by government agencies who want to check you're paying taxes.

This isn't a conspiracy theory. It's how the internet works in 2026. And most people have no idea how much of their daily life is being recorded.

This guide explains what's happening, who's doing it, and what you can do about it — in plain English, without the jargon.

## Part 1: How companies track you

### Your browser is a snitch

Every time you visit a website, your browser hands over information about you: what device you're using, what screen size you have, what fonts are installed, your timezone, and your approximate location. Put all of that together and it creates a "fingerprint" that's almost as unique as your actual fingerprint.

This means that even if you clear your cookies, websites can often still recognise you.

### Cookies: the ones you keep clicking "Accept" on

Those annoying pop-ups asking you to accept cookies? Most people click "Accept all" just to make them go away. What you've just agreed to is letting that website — and often dozens of advertising companies — drop small tracking files on your computer.

These files follow you across the internet. That's why you search for a holiday to Spain and suddenly every website you visit shows you adverts for flights to Malaga.

## Google sees almost everything

Google runs the most popular search engine, the most popular email service (Gmail), the most popular web browser (Chrome), the most popular video site (YouTube), and the most popular phone operating system (Android). If you use any of these, Google has a detailed record of your searches, your emails, your location history, your YouTube viewing habits, and your app usage.

Google also runs Google Analytics, a free tool used by the vast majority of websites to track their visitors. This means Google knows not just what you search for, but which websites you visit afterwards — even ones that have nothing to do with Google.

## Facebook follows you off Facebook

You might think Facebook only knows what you post. In reality, millions of websites have a Facebook "Like" button or Facebook "Pixel" embedded in their pages. Every time you visit one of those sites while logged into Facebook, Facebook records it. They build a profile of your interests, your purchasing habits, and your browsing patterns — all to sell more targeted advertising.

## Your supermarket knows more about you than your doctor

If you use a loyalty card at Tesco, Sainsbury's, or any supermarket, they have a complete record of every item you've ever bought. They know your dietary habits, whether you buy alcohol, whether you've recently bought pregnancy tests or pet food. This data is analysed and used to target you with personalised offers — and sometimes shared with third parties.

## Your phone tracks your every move

Both Apple (iPhone) and Google (Android) record your location continuously. Google has a feature called "Timeline" that shows everywhere you've been, for years. Even if you turn off location services, your phone connects to mobile masts and WiFi networks that reveal your approximate position.

# Part 2: How the government watches you

## The Snoopers' Charter

The Investigatory Powers Act 2016 — nicknamed the "Snoopers' Charter" — gives the UK government sweeping surveillance powers. Under this law:

★ Your internet service provider (BT, Sky, Virgin, etc.) is legally required to store a record of every website you visit for 12 months. Not the content of the pages, but which sites you visited and when.

★ Police, HMRC, and over 40 other government agencies can access these records — often without needing a warrant from a judge.

★ GCHQ (the Government's listening agency) can collect internet traffic in bulk, intercepting communications that pass through the UK's internet cables.

**This is not speculation. It's the law.**

## HMRC's digital detective

If you thought the taxman relied on paper forms and tip-offs, think again. HMRC operates a system called "Connect" — a massive AI-powered platform that cross-references over 55 billion pieces of data from more than 30 sources.

Connect pulls information from:

★ Bank accounts and building society records (UK and 60 overseas countries)

★ Credit and debit card transaction records from Visa and Mastercard

★ Land Registry records (who owns which properties)

★ DVLA records (what car you drive)

★ Online marketplace records (eBay, Amazon, Airbnb, Etsy)

★ Social media posts (yes, really — HMRC confirmed this in 2025)

★ Utility company records

★ Letting agent and tenancy deposit records

The system builds a profile of each taxpayer and looks for inconsistencies. If your declared income is modest but your Instagram shows a new Range Rover and holidays in the Maldives, Connect will flag you for investigation.

In the 2024/25 tax year alone, Connect helped HMRC collect an additional £4.6 billion in tax. Over 90% of HMRC investigations are now triggered by Connect's data analysis rather than random checks or tip-offs.

From April 2026, sole traders and landlords earning over £50,000 must file quarterly digital tax returns under "Making Tax Digital" — giving HMRC even more real-time data to analyse.

## ANPR cameras

Automatic Number Plate Recognition cameras are positioned on roads across the UK. They record every car that passes, along with the time and location. This data is stored for up to two years by the police. That means there is a record of where your car has been, when, for the last two years.

## Your bank reports to HMRC

Banks are required to report interest earned on savings accounts to HMRC. If the interest you earn doesn't match what's on your tax return, Connect spots it instantly. From 2024, online platforms like eBay and Airbnb must report sellers' transactions to HMRC once they exceed certain thresholds.

## The solution: Pecunia Rex Est!

Cash is king. To protect your anonymity and privacy, use cash wherever possible and consider alternatives to bank transactions like barter and bitcoin. Always be aware of cryptocurrency scams and the volatility of these "virtual" assets — they are unregulated, highly speculative, and a favourite tool of fraudsters. If you don't fully understand how cryptocurrency works, don't invest in it.

## Palantir — the company connecting everything together

If the individual surveillance systems above sound worrying on their own, consider what happens when you connect them all together. That's exactly what a company called Palantir does.

Palantir is an American technology company originally funded by the CIA. Its software is designed to take separate databases — health records, tax records, police records, bank records, vehicle records — and join them into a single searchable system. It was built for spy agencies. Now it's embedded across the UK government.

Palantir currently holds at least 34 contracts with UK government bodies worth over £670 million. These include:

★ The NHS — a £330 million contract to build a "Federated Data Platform" connecting patient data across 240 NHS organisations. Your hospital visits, waiting list position, prescriptions, and discharge records — all on one platform run by a company founded by CIA money.

★ The Ministry of Defence — a £240 million contract awarded without competitive tender, helped along by Peter Mandelson's lobbying firm.

★ UK police forces — building AI-powered, real-time data-sharing networks that process sensitive information including people's health, sexual orientation, biometric data, trade union membership, race, religion, and political beliefs. When journalists asked police forces about these contracts, some forces deleted them from public record.

★ The Financial Conduct Authority — given access to sensitive financial crime data.

In the United States, Palantir built the immigration enforcement system used by ICE to track, target, and deport people — including using health data to find them. In 2025, it won a $30 million contract for "ImmigrationOS," a platform designed for near-real-time tracking of deportations.

Why does this matter in the UK? Because Reform UK has already published plans to "automatically share data between the Home Office, NHS, HMRC, DVLA, banks and the police" if it wins power. Palantir's software is purpose-built for exactly this kind of cross-department data sharing. The infrastructure is already being installed.

The British Medical Association — representing over 200,000 doctors — has told its members to limit engagement with Palantir's NHS system. Around 50,000 patients have written to hospital trust boards urging them not to adopt it. More than half of NHS trusts are refusing to use it. But the contracts keep growing.

Palantir also has a history with Cambridge Analytica — the firm that harvested millions of Facebook profiles to influence elections. A whistleblower testified to the UK Parliament that senior Palantir employees worked on the harvested data. Palantir denied it, then admitted an employee had been involved "in a personal capacity."

An internal Swiss Army report expressed fears that Palantir would pass confidential military data to the CIA and NSA. Norway's largest asset manager divested from Palantir over its role in Israeli surveillance of Palestinians.

> **This is not a fringe conspiracy. This is a company with nearly a billion pounds of UK government contracts, access to your health records, your financial records, and your police records — and a track record of building exactly the kind of surveillance systems that civil liberties groups have warned about for decades.**

## Google — the company that knows you best

Google deserves its own section because most people don't realise how much of the internet it controls.

Google runs the world's most popular search engine, email service (Gmail), web browser (Chrome), video platform (YouTube), mobile phone operating system (Android), maps service, cloud storage, and online advertising network. If you use any combination of these — and most people use several — Google has an extraordinarily detailed picture of your life.

But it goes further than the services you use directly. Google Analytics — a free tracking tool — is installed on the vast majority of websites. This means Google knows not just what you search for, but which websites you visit afterwards, even ones that have nothing to do with Google. Google Fonts, another free service, is embedded on millions of websites and sends data back to Google every time a page loads.

YouTube now demands a photo of your face and your date of birth just to create a channel. This is presented as "verification" but it's data collection disguised as security. They don't need your face to host a video about birdwatching.

Google's entire business model is advertising. Everything it offers for free — search, email, maps, YouTube, Chrome, Android — exists to collect data about you so it can sell more targeted advertising. You are not Google's customer. You are Google's product.

> **The safest assumption: if you're logged into a Google account and using Chrome, Google knows essentially everything you do online.**

# Part 3: What you can do about it

You can't disappear from the internet, but you can reduce your exposure significantly.

## Use a VPN

A Virtual Private Network (VPN) encrypts your internet connection and hides your IP address from websites. It also stops your internet provider from seeing which websites you visit. Avoid free VPNs — they make money by selling your data, which defeats the entire purpose.

A VPN does not protect you from Google or Facebook tracking if you're logged into their services. It hides your connection, not your identity.

## Use a private browser

Firefox with Enhanced Tracking Protection blocks many trackers automatically. The Brave browser goes further and blocks almost all advertising trackers by default. Safari on iPhone and Mac has decent built-in protection.

> **Google Chrome is the worst choice for privacy — it's made by the world's largest advertising company.**

## Use a private search engine

DuckDuckGo and Brave Search don't track your searches or build a profile of you. Google records every search you make and uses it to build your advertising profile.

## Don't click "Accept all" on cookies

When a cookie popup appears, look for "Reject all" or "Manage preferences" and turn off everything except "essential" or "necessary" cookies. Yes, it takes a few extra seconds. That's the price of not being tracked across the internet.

## Check your Google account

If you have a Google account, visit myaccount.google.com and look at:

★ "Data & privacy" — you can turn off location history, search history, and YouTube history

★ "My Activity" — this shows you everything Google has recorded about you. It's often eye-opening.

## Be careful with social media

Anything you post publicly on Facebook, Instagram, or Twitter is visible to anyone — including HMRC. Even "friends only" posts can be screenshot and shared. If you wouldn't want the taxman, your employer, or a stranger to see it, don't post it.

## The bottom line

The internet is not a private space. Every click, every search, every purchase creates data that someone is collecting. Companies use it to sell you things. Governments use it to check you're paying taxes. Neither will stop anytime soon.

You don't need to become a hermit or throw away your phone. But you should understand what's happening and make informed choices about what you share. The tools to protect yourself are free and simple — you just need to know they exist.

The generation that grew up with letters, phone calls, and cash had privacy by default. The generation that grew up with the internet has surveillance by default. Understanding the difference is the first step to protecting yourself.

---

## Sources

1. HMRC Connect system — TaxAssist Accountants, November 2025. taxassist.co.uk
2. HMRC Connect — how the taxman is spying on you — THP Chartered Accountants, April 2025. thp.co.uk
3. HMRC uses AI to spy on social media posts — Yahoo News / The Telegraph, August 2025
4. HMRC Connect £4.6 billion additional revenue — Kreston Reeves, January 2026. krestonreeves.com
5. HMRC Connect 55 billion data points, Palantir partnership — Digital Campaign, November 2025
6. Making Tax Digital from April 2026 — TaxWatch UK, December 2025. taxwatchuk.org
7. HMRC expanding AI use — Public Technology, January 2026. publictechnology.net
8. Palantir UK contracts, at least 34 worth £670 million — The Nerve, Carole Cadwalladr, January 2026
9. Palantir NHS FDP £330 million contract — The Register, March 2026. theregister.com
10. Palantir MoD £240 million contract — The Lowdown NHS, April 2026. lowdownnhs.info
11. Peter Mandelson's role — The Lowdown NHS; OpenDemocracy MoD-to-Palantir pipeline report
12. Palantir police surveillance — Liberty Investigates and the i Paper, June 2025
13. Police forces deleted Palantir contracts — Democracy for Sale / NPCC investigation
14. FCA insider concerns — Novara Media, March 2026. novaramedia.com
15. Palantir ImmigrationOS $30M ICE contract — The Small Business Cybersecurity Guy, Feb 2026
16. Reform UK data-sharing plans — Reform UK 'Operation Restoring Justice', August 2025
17. BMA told doctors to limit engagement — Computer Weekly, March 2026
18. 50,000 patients wrote to trust boards — Good Law Project 'Say No to Palantir' campaign
19. More than half of NHS trusts not using FDP — Corporate Watch FOI investigation, August 2025
20. Palantir and Cambridge Analytica — Christopher Wylie testimony to UK Parliament, March 2018
21. Swiss Army fears about Palantir/CIA — Medact briefing, March 2026. medact.org
22. Norway's Storebrand divested from Palantir — Storebrand Asset Management, October 2024
23. Parliamentary Early Day Motion — UK Parliament EDM 65235, February 2026
24. Investigatory Powers Act 2016 — UK legislation. legislation.gov.uk
25. ANPR data retention — UK Surveillance Camera Commissioner guidance

*This guide was written for the community. Share it with anyone who might find it useful.*