Lewis Joseph Feik
Case Project 6-4
Security Awarness

Can you trust your VPN? A 2025 reality check

VPNs don't give you "end-to-end" secrecy. *They create an encrypted tunnel to the VPN operator (typically using TLS for OpenVPN or the WireGuard Noise protocol). Beyond that point, the provider can still see connection metadata (e.g., the destination IP/DNS) unless it is engineered—and audited—not to retain it. That visibility has been abused before.*

When VPNs have failed users

- ***Hola VPN (2015)****: the free, peer-to-peer extension* **sold users' bandwidth** *via its "Luminati" network, enabling botnet-style misuse—about as far from privacy as you can get. PCWorld+1*

- ***Hotspot Shield (2017)****: a detailed* ***FTC complaint*** *alleged undisclosed data practices and traffic redirection for ads that contradicted its privacy promises. cdt.org+2The Register+2*

- ***UFO VPN (2020)****: despite "no-logs" claims, an* **unsecured database leaked 894 GB** *of logs, including plaintext passwords, IPs, and timestamps. BetaNews+2MalwareTips Forums+2*

- ***PureVPN (2017)****: reporting around an FBI case showed how* **connection logs** *can deanonymize users, underscoring why even "metadata only" can be dangerous. ProPrivacy.com*

- ***Facebook's Onavo****: marketed as a VPN, it was used to* ***harvest competitive intelligence*** *and was pulled from Apple's App Store for violating data-collection rules. Ars Technica+2The Verge+2*

Lewis Joseph Feik
Case Project 6-4
Security Awarness

What three reputable VPNs promise (and how to verify)

***Mullvad** (Sweden):*

- ***Terms of Service**: "our policy [is] to **never store any activity logs or metadata**," with minimal data retention overall. Mullvad VPN*

- ***No-logs policy page**: "We do not keep activity logs of any kind," explicitly listing **no traffic, DNS, connection timestamps, IP addresses, or bandwidth logs**. Mullvad VPN*

- ***Real-world verification**: in 2023, Swedish police served a **search warrant**; officers left with **no customer data**. Mullvad VPN+1*

***IVPN** (Gibraltar):*

- ***Privacy Policy**: "We **do not log any data** relating to a user's VPN activit. No traffic logging, **no timestamps**, **no DNS** logging, **no IP** logging." ivpn.net*

- ***Independent audit**: Cure53's **no-log audit** (2019) "concluded with positive verification of the security claims." cure53.de*

***Proton VPN** (Switzerland):*

- ***Privacy Policy / No-logs page**: "We **do not log users' traffic** or the content of communications," and **keep no records** of online activity or session lengths. Proton VPN+1*

- ***Independent verification**: completed its **fourth consecutive no-logs audit** (2025) by Securitum; confirms **no user activity, metadata, or traffic logs** are stored. TechRadar+1*

- ***Legal/trust signals**: Proton documents a 2019 case where it **could not provide logs** because none existed. Proton VPN+1*

Lewis Joseph Feik
Case Project 6-4
Security Awarness

How can you actually verify "no-logs" claims?

1. ***Independent audits*** *(repeatable, scope disclosed): e.g., Proton's annual Securitum audits; IVPN's Cure53 audit.* *TechRadar+1*

2. ***Adversarial tests*** *(raids/seizures): e.g.,* ***Mullvad's 2023 police raid*** *yielded no data; likewise* ***ExpressVPN's Turkey server seizure (2017)*** *found* ***no logs*** *a classic real-world proof.* *Mullvad VPN+2The Verge+2*

3. ***Architecture****: RAM-only servers, minimal or anonymous accounts (e.g.,* ***numbered accounts*** *at Mullvad), and clearly documented handling of payment data.* *Mullvad VPN*

4. ***Transparency reports / canaries*** *and* ***open-source apps*** *(so researchers can validate client behavior).* *Proton VPN*

Are the protections sufficient?

They're ***getting better****, but vigilance matters. The failure cases above show marketing can diverge from practice. The strongest providers pair* ***clear, specific promises*** *("no DNS/traffic/timestamp/IP logs") with* ***audits*** *and* ***incident-tested designs****. Users should not rely on "VPN = anonymity"; instead, choose services that minimize what they can collect by design and prove it regularly.*

Which VPN would I choose—and why?

Mullvad *is my top pick for maximum privacy with the least trust required:* ***no account email, cash accepted****, explicit* ***no-logs in the ToS****, and a* ***police raid that found nothing****.* *Mullvad VPN+2Mullvad VPN+2*
Close runner-up: ***Proton VPN****, thanks to* ***repeat third-party audits*** *and Swiss jurisdiction; if you want open-source apps and frequent independent scrutiny, Proton is excellent.* *TechRadar*
IVPN *also earns trust with a* ***plain-English policy*** *and audit track record another solid choice.* *ivpn.net+1*

Bottom line: *A VPN can still see a lot; the question is whether it* ***retains*** *anything. Pick one that (a)* ***promises specifically what it won't store****, (b)* ***proves it*** *(audits and real-world tests), and (c)* ***collects as little as possible*** *to function. Mullvad, Proton VPN, and IVPN fit that bill unlike the historical counter-examples that turned users into the product.*