An Investigative Report on the OperaGX VPN: Technical Efficacy vs. Corporate Trust

Introduction

This report addresses the central dilemma facing users of the OperaGX browser: the allure of a service marketed as a "free, unlimited, no-log VPN" [1] set against a backdrop of persistent and serious questions regarding its technical reality, data privacy practices, and corporate ownership. The OperaGX browser, with its gamer-centric features and aesthetic, has cultivated a significant user base. A key feature promoted to this audience is its integrated Virtual Private Network (VPN), which promises enhanced privacy and security at no cost and with no data caps.[1]

However, this offering is shadowed by controversy. For years, security experts and privacy advocates have raised concerns that range from the technical—questioning whether the service is a true VPN at all—to the geopolitical, focusing on the implications of Opera's 2016 acquisition by a Chinese consortium. This investigation seeks to cut through the marketing claims and the historical speculation to provide a definitive, evidence-based analysis. The objective is to dissect whether the OperaGX Free VPN is an effective tool for data protection or if the concerns about its technical architecture, data leak vulnerabilities, and ownership structure render it, as the query suggests, "too shady" to be trusted with a user's private data.

This report will systematically deconstruct the service, beginning with its fundamental technology and encryption standards. It will then present an analysis of its practical ability to prevent critical data leaks. Subsequently, it will scrutinize the evolution of Opera's data logging policies, contrasting historical allegations with the company's recent, independently audited claims. Finally, it will conduct a due diligence investigation into Opera's corporate structure and the troubling precedents set by its parent company. By synthesizing these distinct lines of inquiry, this report will deliver a nuanced verdict, empowering users to make an informed decision based on their specific privacy needs and risk tolerance.

Section 1: Technical Architecture: A "VPN" in Name Only?

A foundational analysis of the service offered within the OperaGX browser reveals a critical distinction between its free and paid tiers, a distinction with profound implications for user security. The term "VPN" is applied broadly by Opera, but the underlying technology of the free service differs fundamentally from what a user would typically expect from a true Virtual Private Network.

1.1 The Free Service: A Secure Proxy, Not a True VPN

The core issue at the heart of the OperaGX "Free VPN" is a matter of technical definition and scope. Despite being consistently marketed as a "VPN" [1], the free service is, in technical reality, a browser-based proxy.[3] This is a crucial distinction confirmed by numerous independent security reviews and discussions within technical communities.[7] The service's protection is confined exclusively to the traffic that originates from and is contained within the Opera browser itself.[3] Any other application on the user's computer—be it a P2P file-sharing client like qBittorrent, a standalone email application like Outlook, the Steam client, or even another web browser—remains completely unprotected. The traffic from these applications bypasses the Opera proxy entirely, connecting directly to the internet and exposing the user's real, ISP-assigned IP address.[3]

Furthermore, the free service does not employ dedicated VPN tunneling protocols, which are the cornerstone of a genuine VPN's security architecture. Protocols such as OpenVPN or WireGuard create an encrypted, system-wide tunnel for all of a device's internet traffic. Instead, Opera's free service relies on the standard HTTPS (TLS) protocol for encryption.[3] While TLS provides a strong, encrypted connection between the Opera browser and Opera's proxy server, it lacks the comprehensive, system-level protection and advanced features of a true VPN protocol.[4] This makes its functionality more akin to a browser extension like "HTTPS Everywhere" than a standalone VPN client, as it only secures the data in transit for one specific application.[4]

This discrepancy between marketing and technical reality creates a significant risk. Opera's deliberate and consistent branding of its free proxy as a "VPN" can foster a false sense of security, particularly among users who are not deeply versed in network engineering. The term "VPN" has come to imply comprehensive, device-wide protection in the public consciousness. When users see marketing that promises a "free VPN" with "zero extra steps" [1], they are led to believe their entire digital footprint is being shielded. This misunderstanding can lead to high-risk behavior. For example, a user might enable the "VPN" in OperaGX and then launch a torrent client to download a file, believing their activity is anonymous. In reality, the torrent client's traffic operates completely outside the Opera proxy's protection, broadcasting their real IP address directly to their Internet Service Provider (ISP) and every other peer in the torrent swarm.[3] In this scenario, the marketing choice directly translates into a tangible security vulnerability for the very users the service purports to protect. The "shadiness" is not merely a matter of potential data collection, but also of a fundamental misrepresentation of the service's capabilities that can lead to catastrophic user error.

1.2 Encryption Standards: Strong but Incomplete

On the specific matter of encryption, the service utilizes the industry-standard AES-256 cipher.[2] This is a military-grade symmetric encryption algorithm widely adopted by governments and high-security organizations worldwide. It is considered practically unbreakable by brute-force attacks with current and foreseeable computing technology.[2] When a user enables the free service, their browser traffic is indeed encrypted with this powerful cipher before being sent to Opera's proxy servers.

However, the strength of an encryption cipher is only one component of a comprehensive security solution. Its effectiveness is contingent upon its implementation and scope. As established, the application of AES-256 in the free service is strictly limited to browser traffic. This means that while the data itself is secure in transit between the browser and the proxy, the overall security posture of the user remains weak. The protection is incomplete, leaving all non-browser traffic exposed. The absence of a secure tunneling protocol and other essential security features, which will be discussed later, means that the robust encryption is applied to only a fraction of the user's online activity.

1.3 The Paid "VPN Pro": A Genuine VPN Service

In stark contrast to the free offering, Opera's paid subscription service, "VPN Pro," is a genuine, system-wide VPN.[12] It is engineered to provide the comprehensive protection that users typically associate with the term. VPN Pro protects the entire device, encrypting traffic from all applications on up to six separate devices with a single subscription.[12]

Technologically, VPN Pro is far more advanced. It utilizes modern, secure protocols, including the cutting-edge Lightway protocol.[12] Developed by ExpressVPN and licensed by Opera, Lightway is a lightweight, open-source protocol built on the well-vetted wolfSSL cryptography library. It is designed for high speed, rapid connection establishment, and reliability, particularly on mobile devices where battery life is a concern.[12] Notably, Lightway includes post-quantum protection by default, a forward-looking feature designed to safeguard against the threat of future quantum computers capable of breaking current encryption standards.[12] In addition to Lightway, VPN Pro also supports established and trusted protocols like OpenVPN and IKEv2/IPsec, providing users with flexibility and proven security options.[11]

The infrastructure supporting VPN Pro is also vastly superior. While the free service offers only three or four vague regional server locations (e.g., "Americas," "Europe," "Asia") [13], the paid tier provides access to over 3,000 high-speed servers in 48 distinct locations worldwide.[12] This allows for better performance and more effective bypassing of geo-restrictions. Crucially, VPN Pro includes essential security features absent from the free version, such as a kill switch, which automatically blocks all internet traffic if the VPN connection drops, preventing accidental data exposure.[15]

The profound technical differences between the free and paid services are not accidental. They appear to be part of a deliberate freemium business model designed to upsell users to the paid VPN Pro. The free service offers the *idea* of a VPN—IP masking and basic encryption—but is saddled with significant, well-documented limitations like its browser-only scope, lack of a kill switch, and potential for data leaks. The paid VPN Pro service, in turn, systematically addresses every single one of these deficiencies. It is system-wide, features a kill switch, uses superior protocols, and has a vast server network.[12] This creates a clear and compelling value proposition: users who are initially attracted by the free service and subsequently research its limitations, or experience them firsthand, are naturally guided toward the $4 per month Pro subscription as the "real" solution.[13] From this perspective, the free service functions as a powerful marketing funnel. Its technical shortcomings and "shadiness" are, from a business standpoint, features that highlight the necessity and value of the paid product.

Table 1: Feature Comparison: Opera Services vs. Industry-Standard VPNs

To provide a clear, comparative context, the following table contrasts the features of Opera's free and paid services against a representative industry-leading VPN.

Feature	Opera Free "VPN"	Opera VPN Pro	Representative VPN (e.g., NordVPN, ExpressVPN)
Scope of Protection	Browser-Only Proxy [3]	System-Wide (All Apps) [12]	System-Wide (All Apps)
Primary Protocol	HTTPS/TLS [4]	Lightway, OpenVPN, IKEv2 [12]	WireGuard, OpenVPN, Lightway
Kill Switch	No [3]	Yes [15]	Yes
Audited No-Log Policy	Yes (Deloitte, Sept 2024) [18]	Yes (via Nord partnership) [19]	Yes (Multiple independent audits)
Server Network	3-4 General Regions [13]	3,000+ servers, 48+ locations [12]	5,000-30,000+ servers, 60-100+ countries
Jurisdiction	Norway (Chinese Parent Co.) [20]	Norway (Chinese Parent Co.) [20]	Privacy-Friendly (e.g., Panama, BVI)
Dedicated IP	No [15]	No [15]	Yes (Optional Add-on)
P2P/Torrenting Support	No (Unsafe) [3]	Yes	Yes

Section 2: Data Integrity Analysis: A Test for Leaks

Beyond the theoretical architecture, the practical effectiveness of any privacy tool is determined by its ability to prevent unintentional data leaks that can deanonymize a user. An investigation into Opera's free service reveals vulnerabilities to common leaks that can undermine its core function of identity protection.

2.1 WebRTC Leaks: A Persistent Browser Vulnerability

WebRTC, or Web Real-Time Communication, is a standard API built into modern browsers that enables real-time voice chat, video conferencing, and peer-to-peer file sharing directly within a browser window, without requiring plugins.[22] While useful, this technology carries a well-known vulnerability often referred to as a "WebRTC leak." This leak can allow a specially crafted website to execute a request that bypasses the VPN or proxy tunnel and discovers the user's true public IP address, effectively nullifying the privacy tool's protection.[22]

This vulnerability is not unique to Opera; it is a potential issue in most popular browsers, including Google Chrome and Mozilla Firefox.[22] However, its existence is particularly problematic for a product that markets itself as a privacy solution. Multiple users have reported experiencing IP leaks specifically via WebRTC while using Opera's built-in "VPN".[25] During testing by security researchers, some have found that their real IP address was exposed on leak-testing websites despite the VPN being active.[25]

Crucially, mitigating this risk requires active user intervention. The protection is not enabled by default. Users must navigate to Opera's advanced settings (e.g., by searching opera://settings/?search=WebRTC) and change the WebRTC IP handling policy to "Disable non-proxied UDP".[25] Alternatively, they can install a third-party browser extension specifically designed to manage this, such as "WebRTC Leak Prevent" or "WebRTC Control".[26] Some comprehensive ad-blocking extensions, like uBlock Origin, also include functionality to prevent this type of leak.[25]

This situation reveals a significant flaw in Opera's approach to user privacy. The company markets its free VPN as a simple, one-click solution that requires "zero extra steps" to use.[1] This creates the expectation of out-of-the-box security. However, the reality is that a default browser configuration remains vulnerable to a critical IP leak. A non-technical user, trusting the marketing message, will simply toggle the "VPN" switch and assume they are fully protected. They will have no reason to suspect that they need to delve into advanced configuration menus or research and install specific browser extensions to patch a fundamental vulnerability. Therefore, the service's claim of providing easy and effective privacy is undermined. True protection is not achieved with a simple toggle switch; it is a configuration process that demands a level of technical expertise that contradicts the core marketing message. This gap between promise and reality contributes significantly to the perception of the service being "shady."

2.2 DNS Leaks: Who Sees Your Web History?

Another critical potential point of failure is a DNS leak. The Domain Name System (DNS) acts as the internet's phonebook, translating human-readable domain names (like www.opera.com) into machine-readable IP addresses. A DNS leak occurs when a user's device, despite being connected to a VPN, sends its DNS queries to their default ISP-provided DNS server instead of routing them through the VPN's encrypted tunnel to the VPN's own DNS servers.[29] While this does not expose the

content of the user's internet traffic, it does create a clear, unencrypted log of every single website they visit, which their ISP can see, monitor, and record.[29]

Multiple independent security reviews and user reports indicate that Opera's free "VPN" is susceptible to DNS leaks.[4] A 2024 review from Top10VPN found that the service does not handle DNS requests itself, meaning an unknown third party—most likely the user's ISP—has a log of all DNS requests, which is highly revealing of their browsing activity.[4] In a separate instance, a Reddit user detailed a specific bug where a failed domain lookup would cause the browser to send a direct, unencrypted query to Google's public DNS server (at

8.8.8.8), completely bypassing the VPN tunnel.[30]

This issue is further complicated by another feature within the Opera browser: DNS-over-HTTPS (DoH). DoH is a modern protocol designed to encrypt DNS queries, preventing them from being snooped on in transit.[33] While this is a positive security feature in its own right, its interaction with the built-in "VPN" is confusing and poorly documented. An article from ZDNet notes that on Opera's mobile version, if the VPN is active, the secure DNS feature is automatically disabled, as the VPN is expected to handle DNS resolution securely.[33] However, the situation on desktop is less clear. Users on Opera's forums have reported that even with DoH enabled, DNS leaks can persist.[31] Others have found that enabling DoH can create conflicts with the VPN, leading to widespread connection failures where websites fail to resolve.[34]

This creates a confusing and unpredictable security environment for the user. A logical assumption would be that enabling both the "VPN" and "Secure DNS" would provide the maximum level of privacy. However, the evidence suggests these features can conflict or that one may silently disable the other. There is no clear guidance from Opera on the correct configuration or the operational hierarchy of these two distinct privacy tools. This ambiguity forces users into a frustrating process of trial and error to find a stable configuration. This lack of clarity means a user cannot be confident in their security posture. They may inadvertently create a less secure state by attempting to be *more* secure, which represents a significant design flaw for a product that is supposed to simplify online privacy.

Section 3: The Logging Policy: A Tale of Two Eras

The most critical question bearing on the "shadiness" of the OperaGX VPN is its policy on data logging. A VPN that logs user activity is antithetical to the very concept of privacy. An analysis of Opera's history reveals a stark contradiction between its past reputation and its recent, heavily promoted "no-log" stance, creating a narrative of strategic transformation.

3.1 The Current Stance: The Audited "No-Log" Policy

As of late 2024, Opera's official and unequivocal position is that its free browser VPN is a "strict no-log service".[1] The company's privacy statements and marketing materials explicitly state that it does not log, collect, or store any information related to a user's browsing activity or their originating network address.[2] The policy is clear: "What you do online is your own business".[2]

To add weight to this claim and address long-standing skepticism, Opera commissioned a formal, independent audit of its no-log policy. The audit was conducted by Deloitte, one of the "Big Four" global auditing firms, which has also been trusted to audit the policies of other well-regarded VPN providers.[18] The audit, which took place from June to August 2024, was comprehensive. It involved a thorough review of Opera's VPN infrastructure, an inspection of the technical configurations of its servers, and an analysis of internal policies and documentation.[18]

The results of the audit, announced in September 2024, were positive for Opera. Deloitte's report concluded that they "did not identify any instances" of non-compliance with Opera's stated no-log policy.[18] The auditors confirmed that the IT systems and operational controls were "suitably designed and implemented" to uphold the no-log promise.[19] A crucial part of the report was Opera's own Management Assertion, which stated, "There is no data logging functionality built into the VPN service, and no data whatsoever is collected about users' browsing activity, browsing history, originating network address, or other identifying information".[19] This audit covers the free VPN service across all platforms where it is offered: Opera and OperaGX for desktop, as well as Opera for Android and iOS.[19]

3.2 The Historical Allegations: A Legacy of Distrust

This newly audited stance stands in sharp contrast to the company's reputation for the better part of the previous decade. Prior to the 2024 audit, the consensus among many security experts and privacy advocates was that the free VPN was fundamentally unsafe precisely because of its data collection practices.[3]

Critical analyses, such as a detailed report from CyberInsider, pointed directly to language in Opera's own past privacy policies. These policies allegedly gave the company the right to collect user data to be used for "promotional campaigns and advertising" and to share this data with third-party partners, including data giants like Google and Facebook.[6] A particularly alarming practice highlighted by researchers was the assignment of a unique "device_id" to each browser installation. This identifier was reportedly sent to the proxy server with every browsing request, allowing for the creation of a permanent, linkable record of a user's activity tied to their specific device.[6] This collection of detailed "usage data" linked to a unique ID is the operational model of an advertising company, not a privacy service.[6]

This perception was widespread and deeply entrenched. Users on forums like Reddit actively warned others that Opera's own policy "says that it logs all your information," which "pretty much defeats the purpose of a VPN".[5] For years, the lack of an independent audit was a major red flag highlighted in nearly every critical review of the service, with publications like Forbes noting that while Opera claimed a no-logs policy, it had not been independently verified.[15] This fueled the pervasive suspicion that for this "free" service, the user's data was the actual product being monetized.[5]

3.3 Synthesis: A Strategic Reversal or a Genuine Reformation?

The 2024 Deloitte audit cannot be viewed in a vacuum. It represents a significant and calculated strategic maneuver by Opera to neutralize years of damaging criticism and fundamentally reshape its public image. The timing and nature of the audit suggest it is a direct response to a long-standing reputational liability. For years, the primary arguments against trusting the Opera VPN were its vague privacy policy, the suspicion of data logging for monetization, and the glaring absence of independent verification.[5] This was a major obstacle to being considered a legitimate privacy tool.

The announcement of a successful no-log audit by a reputable firm like Deloitte directly addresses the single most persistent and damaging criticism that has been leveled against the service. It provides a powerful piece of third-party evidence that Opera can now use to counter the historical allegations. This allows the company to attempt to rewrite its narrative from that of a "shady data collector" to a "verified no-log provider."

Therefore, the audit can be interpreted as a calculated business decision aimed at rebuilding trust and repairing a damaged brand. While the findings themselves are positive and attest to the current state of Opera's systems, the context in which the audit was commissioned is crucial. The user is left to decide whether this represents a genuine, top-to-bottom reformation of corporate ethics and a newfound commitment to user privacy, or a sophisticated and necessary public relations maneuver to shed a toxic reputation and make its products more commercially viable.

Table 2: Timeline of Opera's Privacy Posture and Ownership

This timeline provides essential context, illustrating the long period of user distrust followed by a very recent, major effort to build credibility.

Date	Event	Implication for Trust	Source(s)
1995	Opera founded as an independent Norwegian company.	High trust; operates under strong European privacy norms.	20
July 2016	Opera's browser business is sold to a Chinese consortium led by Kunlun Tech for $600 million.	Major blow to trust; introduces concerns about Chinese government influence and data privacy.	20
2016-2023	A period of intense criticism regarding data logging, use of unique device IDs for tracking, and monetization of user data for ads.	Low trust; widespread perception that the "free" VPN's business model is based on user data collection.	4
March 2019	Opera's parent company, Kunlun Tech, is forced by the U.S. government (CFIUS) to sell the Grindr app over national security data concerns.	Extremely low trust; establishes a documented precedent of Kunlun's control over user data being deemed an unacceptable national security risk by a Western government.	38
Sept 2024	Opera announces the successful completion of a "no-log" audit for its free browser VPN, conducted by Deloitte.	A significant strategic move to rebuild trust; provides the first piece of independent verification for its no-log claims.	18

Section 4: The Ownership Question: The Shadow of Kunlun Tech

The most profound and difficult-to-mitigate concerns surrounding the OperaGX VPN stem from its corporate ownership. This section moves beyond technical specifications and logging policies to conduct a due diligence investigation into Opera's corporate structure, focusing on the geopolitical risks associated with its parent company—a risk that lies at the very heart of the "shady" question.

4.1 Corporate Structure: A Jurisdictional Duality

Opera presents itself to the world with a dual identity. On paper, Opera Limited is a Norwegian company, with its headquarters in Oslo, Norway, and it is publicly traded on the American NASDAQ stock exchange.[20] The company frequently emphasizes this Norwegian identity, stating that it operates under Norwegian and, by extension, stringent European privacy laws, including the General Data Protection Regulation (GDPR). It also asserts that all user data is processed and stored on servers located within Europe.[2] This is its primary legal defense against privacy concerns.

However, this European identity is overlaid with a controlling foreign interest. Since the 2016 acquisition, Opera has been majority-owned by Beijing Kunlun Tech Co., Ltd., a publicly-traded Chinese technology and gaming company.[20] The connection is not merely financial; it is operational. The Chairman and CEO of Opera, Mr. James Yahui Zhou, is simultaneously the controlling shareholder and CEO of the parent company, Kunlun Tech.[20] This creates a direct and undeniable command-and-control link between Opera's highest level of management and its Chinese parent company.

4.2 A Troubling Precedent: The Kunlun-Grindr-CFIUS Case

The potential risks associated with this ownership structure are not theoretical. They have been tested and validated in a high-profile international incident involving Opera's parent company. In 2019, the Committee on Foreign Investment in the United

States (CFIUS)—a powerful and secretive U.S. government body that reviews foreign acquisitions for national security risks—took the extraordinary step of forcing Kunlun Tech to sell Grindr, a popular gay dating and social networking app that Kunlun had acquired in stages between 2016 and 2018.[38]

The rationale for this forced divestiture was national security. CFIUS determined that Kunlun's ownership of Grindr posed an unacceptable risk to the United States. The committee was concerned that the Chinese government could potentially compel Kunlun to provide access to the vast trove of sensitive personal data collected by the app. This data included the real-time location, private messages, personal photos, and even the HIV status of millions of American users.[38] U.S. officials feared this information could be weaponized for espionage or blackmail, particularly against government employees and military personnel who might use the app.[38] This case is not a mere allegation or a conspiracy theory; it is a documented, official action by a major Western government that concluded Kunlun Tech's control over sensitive user data was an intolerable national security threat.[38]

4.3 The Legal Framework: China's National Intelligence Law

The concerns that drove the CFIUS decision are rooted in China's broad and powerful national security legal framework. China's 2017 National Intelligence Law, in particular, contains articles that are a source of profound concern for international governments and corporations. Article 7 of the law states: "All organizations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with law".[45] This duty is not optional. Article 14 of the same law grants Chinese state intelligence agencies the authority to demand this cooperation from any relevant organization or citizen.[46]

The expert interpretation of this law among Western legal and intelligence analysts is that it could be used to legally compel a Chinese company like Kunlun Tech to hand over any and all data to which it has access, regardless of where that data is physically stored or which country's citizens it pertains to.[45] The law effectively deputizes Chinese companies, making them potential instruments of state intelligence gathering.

4.4 Synthesis: Weighing Jurisdictional Defense Against Geopolitical Risk

This analysis brings the central conflict into sharp focus. Opera's primary defense is its "jurisdictional firewall": the argument that it is a Norwegian entity, governed by GDPR, and therefore user data is safe.[2] This is a legal argument based on corporate structure and data residency. However, this legal shield may not be robust enough to withstand the practical realities of state-level pressure exerted on its Chinese parent company, which is subject to a completely different and overriding legal framework.

The user's decision to trust Opera's free VPN is therefore not simply a technical assessment. It is a judgment on geopolitical power dynamics. The Grindr case serves as a crucial, real-world stress test of this very conflict.[38] In that instance, the U.S. government decided that the geopolitical threat—the potential for Chinese state access to data via Kunlun—outweighed any and all legal protections or privacy policies the company may have had in place.

While the recent Deloitte audit confirms that Opera's *current systems* are configured not to log user data [19], this audit is a snapshot in time. It verifies a technical state but cannot audit future intent or future compulsion. China's National Intelligence Law could, in theory, be used to compel Kunlun to pressure Opera's leadership to

change its systems, to install a new monitoring capability, or to provide access in a way that bypasses normal logging functions. Such a directive would be secret and not subject to public disclosure or audit.

Therefore, the user is not just trusting Opera's current policy or its recent audit. They are being asked to trust that the Norwegian legal entity can, and will, successfully resist any and all future pressure from its Chinese parent company, which may itself be acting under a legal mandate from the Chinese state. This is an unprovable and significant structural risk that cannot be mitigated by any technical audit. This inherent, unresolvable risk, born from the ownership model, is the deepest source of the service's "shadiness."

Section 5: Final Verdict and Recommendations

Synthesizing the comprehensive analysis of its technical architecture, data integrity, logging policies, and corporate ownership, this report can now provide a direct, multi-faceted answer to the user's query and offer actionable advice based on different user risk profiles.

5.1 On Effectiveness: Is it a Good Data Protection Tool?

Verdict: No, the OperaGX Free VPN is not an effective tool for comprehensive data protection.

The service is fundamentally a browser-only proxy, not a true VPN. This architectural limitation means it fails to protect any traffic outside of the OperaGX browser itself. Furthermore, its demonstrated vulnerability to both DNS and WebRTC leaks, which require manual user intervention to mitigate, means that even its in-browser protection is not reliable out-of-the-box.

Acceptable Use Cases:

- **Casual IP Masking:** For non-critical activities on a trusted network where the sole goal is to mask an IP address from a website.
- **Bypassing Simple Geo-Restrictions:** For accessing content on platforms like YouTube that may be unavailable in a user's region, where the stakes of discovery are low.[3]
- **Basic Encryption on Public Wi-Fi:** For adding a thin layer of encryption to non-sensitive browsing (e.g., reading news) at a coffee shop or airport.

Unacceptable and Dangerous Use Cases:

- **P2P File Sharing / Torrenting:** Using the service for this purpose is extremely risky, as it leaves the traffic from the torrent client completely exposed, revealing the user's real IP address to their ISP and all peers.[3]
- **Circumventing Sophisticated Censorship:** The service lacks the advanced obfuscation features necessary to bypass robust state-level firewalls or censorship regimes.
- **Protecting Sensitive Activities:** It should never be used for protecting sensitive financial transactions, confidential business communications, or any activity where a data leak could have serious consequences.
- **Protection from Targeted Adversaries:** The service lacks the security features and architectural integrity to protect a user from a determined, targeted

adversary.

5.2 On Trustworthiness: Is it "Too Shady"?

Verdict: Yes, for any user for whom privacy and data security are primary concerns, the service carries an unacceptably high level of "shadiness" due to unmitigable structural risks.

This conclusion is based on a balance of positive and negative factors.

Factors for Trust (The Pro-Opera Case):

- The September 2024 no-log audit by Deloitte is a significant and positive development. It provides credible, third-party verification that the current technical systems are not designed to log user activity.[18]
- The company's legal domicile in Norway subjects it to the strong data protection regulations of the GDPR, which offers users a robust legal framework for privacy rights.[2]

Factors for Distrust (The "Shady" Case):

- **Misleading Marketing:** The service is technically a proxy but is deliberately and consistently marketed as a "VPN," which creates a false sense of security and can lead to dangerous user errors.[3]
- **Damaging Precedent of Parent Company:** The parent company, Kunlun Tech, has a documented history—the forced sale of Grindr—of being officially deemed a national security risk by the U.S. government specifically because of its control over sensitive user data.[38] This is a powerful indictment of the parent company's suitability as a custodian of private information.
- **Geopolitical and Legal Risk:** The parent company's location in China subjects it to the National Intelligence Law, creating a potential, legally-enforceable backdoor for state intelligence to access data. This is a structural risk that cannot be audited away and overrides any promises made by the Norwegian subsidiary.[45]

5.3 Final Recommendations Based on User Profiles

The decision of whether to use the OperaGX Free VPN ultimately depends on an individual's specific needs and tolerance for risk.

- **For the Casual User:**
    - **Profile:** A user whose primary goal is convenience. They want to watch a region-locked video, bypass a simple website block at school or work, or feel slightly safer on public Wi-Fi for casual browsing. Their threat model does not include targeted surveillance or serious repercussions for IP exposure.
    - **Recommendation:** The OperaGX Free VPN is likely a **sufficient and convenient** tool for these low-stakes activities. The user should be aware that it only protects their browser traffic and should not be used for anything sensitive. The geopolitical risks, while real, are unlikely to manifest in a way that impacts this user profile directly.
- **For the Privacy-Aware User:**
    - **Profile:** A user who is actively trying to minimize their digital footprint. They are concerned about tracking by their ISP, large tech companies, and advertisers. They value general online anonymity and want a reliable tool to protect their day-to-day browsing.
    - **Recommendation:** This service should be **avoided**. The combination of its proxy-only architecture, the potential for IP and DNS leaks, and the serious, unmitigable risks associated with its corporate ownership makes it an unreliable and untrustworthy choice for someone who genuinely values privacy. This user would be far better served by investing in a reputable, independently audited, standalone VPN service based in a privacy-friendly jurisdiction.[4]
- **For the High-Risk User:**
    - **Profile:** A user whose activities could attract targeted attention or have serious consequences if their identity were exposed. This includes journalists, activists, whistleblowers, individuals living under repressive regimes, or anyone engaging in activities like P2P file-sharing where IP exposure can lead to legal or financial penalties.
    - **Recommendation:** Using the OperaGX Free VPN is **dangerous and must be avoided at all costs**. The technical limitations are severe, and the profound structural risks related to its ownership make it entirely unsuitable for any high-stakes privacy and security needs. For this user, relying on this service would be a critical security failure.

Works cited

1. Free VPN in GX | Unlimited secure browser VPN | Opera GX, accessed July 8,

2025, https://www.opera.com/gx/features/free-vpn
2. Why browsing with Opera's VPN is safer | Opera Security, accessed July 8, 2025, https://blogs.opera.com/security/2023/02/opera-vpn-is-safe/
3. Opera VPN Review – Is This Free VPN Worth the Risk? - Cybernews, accessed July 8, 2025, https://cybernews.com/best-vpn/opera-vpn-review/
4. Opera Free VPN Review: Why It's Not Safe and Should Be Avoided - Top10VPN, accessed July 8, 2025, https://www.top10vpn.com/guides/is-opera-vpn-safe/
5. Is the Opera browser built-in VPN safe? : r/PiratedGames - Reddit, accessed July 8, 2025, https://www.reddit.com/r/PiratedGames/comments/eqv655/is_the_opera_browser_builtin_vpn_safe/
6. Opera VPN Review 2025 — Data Collection Tool in Disguise? - CyberInsider, accessed July 8, 2025, https://cyberinsider.com/vpn/reviews/opera-vpn/
7. Is the Opera VPN a true VPN or just a proxy - Opera forums, accessed July 8, 2025, https://forums.opera.com/topic/30061/is-the-opera-vpn-a-true-vpn-or-just-a-proxy
8. is the VPN a true encrypted VPN or just a proxy? - Opera forums, accessed July 8, 2025, https://forums.opera.com/topic/35383/is-the-vpn-a-true-encrypted-vpn-or-just-a-proxy
9. Is Opera's "VPN" protecting me from snooping? : r/operabrowser - Reddit, accessed July 8, 2025, https://www.reddit.com/r/operabrowser/comments/672p7l/is_operas_vpn_protecting_me_from_snooping/
10. Opera GX VPN Mobile - Trajectory Hub, accessed July 8, 2025, https://trajdash.usc.edu/opera-gx-vpn-mobile
11. Unveiling The Truth: Does Opera VPN Encrypt Your Data? - Newsoftwares.net Blog, accessed July 8, 2025, https://www.newsoftwares.net/blog/truth-does-opera-vpn-encrypt-your-data/
12. Opera unveils revamped VPN Pro, its premium VPN service offering faster speeds, improved privacy and security, and more locations worldwide - PR Newswire, accessed July 8, 2025, https://www.prnewswire.com/news-releases/opera-unveils-revamped-vpn-pro-its-premium-vpn-service-offering-faster-speeds-improved-privacy-and-security-and-more-locations-worldwide-302495537.html
13. Opera VPN | Free VPN | VPN Pro | Opera, accessed July 8, 2025, https://www.opera.com/features/vpn
14. Opera VPN Pro | Premium VPN | Opera Browser, accessed July 8, 2025, https://www.opera.com/features/vpn-pro
15. Opera VPN Review: Is It Safe To Use In 2025 – Forbes Advisor INDIA, accessed July 8, 2025, https://www.forbes.com/advisor/in/business/software/opera-vpn-review/
16. Opera Limited's VPN Pro: A Secure Browsing Play in the Cybersecurity Surge - AInvest, accessed July 8, 2025,

https://www.ainvest.com/news/opera-limited-vpn-pro-secure-browsing-play-cybersecurity-surge-2507/

17. 5 Opera GX Mobile VPN Tips - AceNet Hub, accessed July 8, 2025, https://www4.acenet.edu/opera-gx-mobile-vpn
18. Opera reaffirms its commitment to privacy with an independent no ..., accessed July 8, 2025, https://press.opera.com/2024/09/25/opera-reaffirms-its-commitment-to-privacy-with-an-independent-no-log-audit-of-its-free-browser-vpn/
19. Protecting your privacy: Opera has completed an independent no ..., accessed July 8, 2025, https://blogs.opera.com/security/2024/09/opera-free-browser-vpn-no-log-audit-deloitte/
20. Opera (company) - Wikipedia, accessed July 8, 2025, https://en.wikipedia.org/wiki/Opera_(company)
21. Is Opera GX Spyware? Here's What You Need to Know - Comparitech, accessed July 8, 2025, https://www.comparitech.com/blog/information-security/is-opera-gx-spyware/
22. How to Fix WebRTC Leaks (Solutions for ALL Browsers) - CyberInsider, accessed July 8, 2025, https://cyberinsider.com/webrtc-leaks/
23. WebRTC leak: how to test & prevent IP leaks - Surfshark, accessed July 8, 2025, https://surfshark.com/webrtc-leak-test
24. WebRTC Leaks: A Complete Guide - Security.org, accessed July 8, 2025, https://www.security.org/vpn/webrtc-leak/
25. IP leak using Opera VPN, accessed July 8, 2025, https://forums.opera.com/topic/22939/ip-leak-using-opera-vpn
26. Here is How To Disable WebRTC in Opera to Prevent Leaking Your IP while using the built in VPN, accessed July 8, 2025, https://forums.opera.com/topic/14850/here-is-how-to-disable-webrtc-in-opera-to-prevent-leaking-your-ip-while-using-the-built-in-vpn
27. WebRTC Protect extension - Opera add-ons, accessed July 8, 2025, https://addons.opera.com/en/extensions/details/webrtc-protect/
28. WebRTC Control extension - Opera add-ons, accessed July 8, 2025, https://addons.opera.com/en/extensions/details/webrtc-control/
29. VPN Leak Test, accessed July 8, 2025, https://www.astrill.com/vpn-leak-test
30. Bug: DNS leak for Opera's VPN feature : r/operabrowser - Reddit, accessed July 8, 2025, https://www.reddit.com/r/operabrowser/comments/m8ldm8/bug_dns_leak_for_operas_vpn_feature/
31. Secure DNS Improvements for Opera Browser with AI, accessed July 8, 2025, https://forums.opera.com/topic/75429/secure-dns-improvements-for-opera-browser-with-ai
32. Opera always leak my Real IP : r/operabrowser - Reddit, accessed July 8, 2025, https://www.reddit.com/r/operabrowser/comments/idfzh3/opera_always_leak_my_real_ip/
33. How to enable DNS over HTTPS in Opera | ZDNET, accessed July 8, 2025,

https://www.zdnet.com/article/how-to-enable-dns-over-https-in-opera/

34. When VPN is Enabled Opera Cannot Connect to Web : r/operabrowser - Reddit, accessed July 8, 2025, https://www.reddit.com/r/operabrowser/comments/1joha4q/when_vpn_is_enabled_opera_cannot_connect_to_web/
35. Transparency Report - Opera Security Team, accessed July 8, 2025, https://security.opera.com/en/opera-transparency-report/
36. Opera (web browser) - Wikipedia, accessed July 8, 2025, https://en.wikipedia.org/wiki/Opera_(web_browser)
37. Opera browser sold to a Chinese consortium for $600 million - Engadget, accessed July 8, 2025, https://www.engadget.com/2016-07-18-opera-browser-sold-to-a-chinese-consortium-for-600-million.html
38. CFIUS Forces Kunlun to Unwind 2016 Acquisition of Grindr Over Concerns About the Protection of Sensitive Personal Data | Cleary Cybersecurity and Privacy Watch, accessed July 8, 2025, https://www.clearycyberwatch.com/2019/04/cfius-forces-kunlun-to-unwind-2016-acquisition-of-grindr-over-concerns-about-the-protection-of-sensitive-personal-data/
39. Chinese Acquire Social Media Platforms to Spy? - Lee Neubecker, accessed July 8, 2025, https://leeneubecker.com/chinese-acquire-social-media/
40. Opera Software 2025 Company Profile: Stock Performance & Earnings | PitchBook, accessed July 8, 2025, https://pitchbook.com/profiles/company/230458-69
41. Opera Ltd Company Profile - Overview - GlobalData, accessed July 8, 2025, https://www.globaldata.com/company-profile/opera-ltd/
42. Management Team | Opera Limited, accessed July 8, 2025, https://investor.opera.com/shareholders-governance/management/
43. Opera is spyware? : r/operabrowser - Reddit, accessed July 8, 2025, https://www.reddit.com/r/operabrowser/comments/ajmbox/opera_is_spyware/
44. Is it a threat to US security that China owns Grindr, a gay dating app? - Brookings Institution, accessed July 8, 2025, https://www.brookings.edu/articles/is-it-a-threat-to-us-security-that-china-owns-grindr-a-gay-dating-app/
45. China has law requiring businesses and persons oversees to get secrets from host countries and their businesses for China's government - Jeff Newman Law, accessed July 8, 2025, https://jeffnewmanlaw.com/china-has-law-requires-businesses-and-persons-oversees-to-get-secrets-from-host-countries-and-their-businesses-for-cginas-government/
46. PRC National Intelligence Law (as amended in 2018), accessed July 8, 2025, https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/
47. China National Security Laws - Office of Innovative Technologies, accessed July 8, 2025,

https://oit.utk.edu/wp-content/uploads/China-National-Security-Laws.pdf

48. en.wikipedia.org, accessed July 8, 2025, https://en.wikipedia.org/wiki/National_Intelligence_Law_of_the_People%27s_Republic_of_China#:~:text=Experts%20argue%20that%20the%20law,country%20that%20data%20came%20from.
49. IS OPERA VPN SAFE TO USE? What You Need to Know About This VPN Provider's Security Features - YouTube, accessed July 8, 2025, https://www.youtube.com/watch?v=5yRStP3I_Xs