

Report: Google, Russian Propaganda, and European Compliance

Executive Summary

This report examines Google's role in the dissemination of Russian propaganda, its advertising revenues in Russia, and its compliance challenges with European regulations. Drawing on multiple journalistic sources, it highlights the tension between Google's global business model and Europe's demand for transparency, privacy, and sovereignty.

1. Google and Russian Propaganda Channels

- Institute for Strategic Dialogue (ISD) reports that despite EU sanctions, Russian propaganda websites remain accessible in Europe.
 - One reason is the use of Google Public DNS and Cloudflare DNS, which allow users to bypass national blocks.
 - iStories article “How Google helps Russian propaganda” (March 2023) explains how Google’s infrastructure indirectly facilitates the spread of Kremlin narratives source: iStories.
-

2. Google’s Advertising Revenues in Russia

- According to TAdviser, Google earned significant revenue from advertising in Russia, even after the start of the war in Ukraine.
 - Ads purchased by Russian companies and state-linked actors contributed to Google’s global profits.
 - This raises questions about whether Google prioritized revenue over compliance with sanctions [source: TAdviser].
-

3. European Concerns and Regulatory Pressure

- The European Union has repeatedly fined Google for GDPR violations and antitrust practices.

- The MSN report on the EU antitrust probe (2024) shows regulators investigating whether Google's anti-spam policies unfairly affect publishers [【source: MSN】](#).
 - The lack of transparency in Google's VPN and DNS services — particularly the inability to see entry/exit nodes — is seen as non-compliance with European standards.
 - Archyde article "Europe's Public DNS: A Google Alternative" highlights the push for Quad9 and NextDNS as GDPR-compliant alternatives [【source: Archyde】](#).
-

4. Alternatives: Quad9 and NextDNS

- Quad9 (Switzerland): blocks malicious domains, respects privacy, and complies with European jurisdiction.
 - NextDNS (EU-based): offers granular filtering, parental controls, and GDPR compliance.
 - Both are considered superior to Google DNS in terms of transparency, privacy, and sovereignty [【source: Archyde】](#).
-

5. Critical Observations

- Google's reluctance to fully comply with European standards is suspicious, especially given its revenues from Russian Ads.
 - The combination of economic gain and infrastructural opacity undermines trust in Google's role as a neutral technology provider.
 - Europe's response — fines, investigations, and promotion of alternatives — reflects a growing demand for digital sovereignty.
-

Conclusion

Google's infrastructure and advertising practices have indirectly supported the spread of Russian propaganda in Europe, while its VPN and DNS services raise compliance concerns under GDPR. The company's global revenue model, including profits from Russia, contrasts sharply with Europe's push for transparency and sovereignty. Alternatives like Quad9 and NextDNS demonstrate that compliant, privacy-focused solutions are possible — and increasingly necessary.

References

- MSN: EU launches antitrust probe into Google's anti-spam policy
- iStories: How Google helps Russian propaganda
- TAdviser: Google's revenue and profits in Russia
- Archyde: Europe's Public DNS — A Google Alternative