platforma

Big Tech and Russian Wartime Censorship: 2022–2025

Executive summary

Since Russia's full-scale invasion of Ukraine in 2022, U.S. and Western technology companies have operated under sustained pressure from Russian censorship authorities, Western sanctions regimes, and reputational risk. Evidence from platform transparency reports, independent media, and civil society demonstrates a consistent pattern: major technology companies have frequently over-complied with Russian censorship demands, applied opaque enforcement practices, and failed to mitigate the downstream effects of state repression on their platforms.

Rather than limiting the Kremlin's information control, these practices have often reinforced Russian wartime censorship, weakened independent media and civil society, and reduced access to reliable information for users inside Russia. At the same time, pro-Kremlin narratives have remained widely accessible and algorithmically amplified.

These outcomes run counter to core EU foreign policy objectives, including support for free expression, independent journalism, and access to information in authoritarian environments. Absent clearer guardrails and accountability, current compliance practices risk enabling Russia's long-term digital isolation strategy while setting harmful precedents for other authoritarian states.

Compliance with Russian censorship demands

Major technology companies have largely treated Russian censorship laws – such as bans on "discrediting the army," "fake news," "extremism," and VPN usage – as routine legal obligations rather than as abusive measures incompatible with international human rights standards. Platforms continued to process takedown and restriction requests from Russian authorities as ordinary legal demands, with little public evidence of legal challenges, principled refusals, or coordinated resistance.

Although companies pursued different compliance strategies, the cumulative effect was similar: independent information was restricted, while state censorship was operationalized through private platforms.

- In 2024, the number of items Russian authorities requested Google to remove reached 784,000—double the figure from the period before the full-scale invasion. Authorities also issued 355 deindexing requests targeting approximately 1.4 million URLs, with Google removing between 53 and 61 percent of the affected links. These actions primarily involved content removal, deindexing, or geo-blocking of anti-war reporting, information on mobilization and conscription, legal guidance on draft resistance, and independent journalism labeled "extremist" or "foreign agent." Google's strategy of partial compliance ultimately failed to preserve YouTube's accessibility in Russia, and the platform was throttled and fully blocked in 2024–2025.
- Meta restricted more than 1,700 pieces of content in early 2022 in response to Russian requests. However, after refusing broader censorship demands related to war coverage, Facebook and Instagram were designated "extremist" and blocked nationwide. While Meta demonstrated partial resistance, it did not implement mitigation strategies to preserve access to independent information following the blocks.
- X (formerly Twitter) showed comparatively low compliance with Russian takedown demands and did not systematically remove war-related content. As a result, the platform was throttled and later effectively blocked. This case illustrates that resistance was possible – but

came at the cost of market access, with no visible U.S. government support for companies choosing this path.

- Apple has taken the most consistently compliant approach. Between 2023 and 2025, Apple removed or restricted content across the App Store, Apple Podcasts, and Apple Music in response to demands from Roskomnadzor and other Russian authorities. This included removal of Russian-language news apps (RFE/RL's Svoboda and Current Time), independent news podcasts (Meduza, Kholod, BBC Russian Service, The Insider, Echo of Moscow), and the blocking or removal of music by artists later designated as "extremist." These actions significantly reduced access to independent journalism for Russian users across Apple's ecosystem.

A particularly consequential divergence concerns tools used to circumvent digital repression. In 2024-2025, Apple removed at least 98 VPN applications from the App Store in Russia, substantially tightening information control. By contrast, Google resisted more than 200 Roskomnadzor requests to remove VPN apps, retaining most of them in Google Play. Both platforms remain accessible in Russia.

Blocking decisions in Russia appear to be driven primarily by the availability of domestic substitutes, not by a platform's willingness to comply with censorship demands. Over-compliance has therefore failed to prevent blocking while contributing to the normalization of state censorship. In early December, it became known that Apple's Facetime messenger had also been blocked. At the same time, the company continues to lose market share in the Russian mobile technology market to Chinese manufacturers. Apple's market share fell by 6% from January–September 2025 compared to the same period in 2024.

Algorithmic reinforcement of state censorship

Platform algorithms have compounded the effects of state censorship. When Russian authorities block independent media websites, user access and engagement decline. Recommendation and search algorithms interpret these signals as reduced relevance, leading to further down-ranking and suppression - effectively extending state censorship through automated systems.

Google Search and Discover demoted independent outlets after they were blocked domestically, while continuing to surface Kremlin-aligned sources, including outlets linked to sanctioned individuals. Platforms have provided only aggregate transparency, offering no meaningful explanations of individual enforcement actions or algorithmic impacts.

Independent media outlets reported sudden, unexplained drops in reach ("shadow bans"), inconsistent or automated responses to appeals, and an absence of effective remedies. Platforms have not adjusted their systems to account for censorship-driven distortions in authoritarian environments.

Over-compliance under sanctions and blanket service restrictions

In parallel, technology companies and service providers imposed blanket restrictions that exceeded U.S. sanctions requirements and disproportionately harmed independent media and civil society rather than the Russian state.

Google and Meta suspended advertising and monetization services in Russia, including YouTube monetization and self-funded ad promotion for anti-war content. Other providers - including Mailchimp, Slack, Adobe, Microsoft services, and nonprofit support programs such as TechSoup – ceased services to Russian independent media and NGOs.

As a result, independent outlets and civil society organizations lost access to essential infrastructure, productivity tools, and – in many cases – their last remaining legal revenue streams. These outcomes undermined the resilience of pro-democracy actors while leaving state-aligned media largely unaffected.

Policy implications

The cumulative effect of over-compliance, opaque enforcement, and algorithmic neglect has been to outsource elements of Russian wartime censorship to U.S. companies, weakening access to independent information.

To address these risks, EU policymakers could consider:

- **Requiring enhanced transparency on bigtech compliance with takedown requests from authoritarian governments**, including reporting on algorithmic impacts in censored environments and the rationale for enforcement decisions. This should include establishing special processing standards for requests originating from authoritarian states, recognizing the high likelihood of abuse.
- **Developing advisory policies for European tech companies** to adopt their own policies on blocking information/ applications and disclosing user information at the request of digitally authoritarian countries, including Russia.
- **Clarifying sanctions exemptions** to explicitly cover SaaS tools for independent media and nonprofits, VPN services, app distribution, and advertising tools - ensuring that sanctions implementation aligns with enforcer`s intent and does not inadvertently strengthen authoritarian information control.
- **EU institutions should create safeguard access to anti-censorship technologies** and ensure that access to anti-censorship tools is neither blocked, criminalized, nor unduly restricted. Any regulatory or enforcement measures must align with international human rights standards of legality, necessity and proportionality. Policymakers should engage in structured consultations with the private sector, civil society and the technical community to evaluate the potential impact of proposed actions. The EU should avoid adopting or promoting legislation that imposes excessive registration, data retention, or content control obligations, digital discrimination as these measures risk undermining privacy, security and the effectiveness of anti-censorship technologies. The biggest challenge in RU right now are local/regional internet shutdowns (+white lists). These make the situation much more complicated than before, as many advanced anti-censorship tools will simply not work.
- **Establishing and maintaining a permanent European Digital Rights Fund (EDRF)** to ensure Europe's digital sovereignty and Internet freedoms for supporting projects in the areas of anti-censorship solutions, privacy, fact-checking groups and digital activism to provide citizens with access to circumvention tools, such as VPNs and encrypted messaging services, to bypass Internet restrictions and to support the creation of privacy technologies and more.
- **Promote and reinforce the multi-stakeholder model of Internet governance**. Active collaboration with the private sector, civil society, academia and the technical community is essential for governments seeking to understand and effectively address developments in anti-censorship and encryption. Governments should prioritise deeper engagement with these actors, especially civil society groups and advocates in contexts where such technologies are vital for resisting digital repression. This includes participation in existing multi-stakeholder platforms such as the Freedom Online Coalition, the Internet Governance Forum (IGF) and its regional counterparts.

- **Strengthen international engagement to safeguard access to anti-censorship and end-to-end encryption tools.** EU institutions should integrate the protection of these technologies into their cyber and digital diplomacy agendas. They should actively advocate for anti-censorship and end-to-end encryption within global frameworks such as the UN Global Digital Compact (GDC), the Digital Freedom Initiative (DFI), and the WSIS+20 Review Process. EU institutions should also promote dialogue on the security, economic, and human rights benefits of these tools, countering disproportionate restrictions in bilateral discussions, multilateral platforms like the Freedom Online Coalition, and, where needed, through the establishment of new alliances.

Find more forecasts in the RKS Global analytical note “Scanning the Horizons of Censorship to 2028” at this link: https://rks.global/en/research/horizon/

***

This policy paper was prepared by Roskomsvoboda.