

VPNs at Risk: Talking Points



Secure Networking, Privacy, and the Consequences of VPN Restrictions

The Big Picture

Virtual Private Networks (VPNs) create encrypted connections across untrusted networks. Long before consumer services became widespread, businesses and governments used VPNs to connect employees, offices, and protected systems. Today, the same capabilities support enterprise cybersecurity and help individuals protect communications and access information.

Key Risks

- Blocking shared protocols or infrastructure can disrupt lawful enterprise and individual VPN uses.
- Retention requirements can undermine privacy-focused VPN architectures and increase exposure of sensitive data.
- VPN restrictions can push users toward less secure services and burden vulnerable communities.
- Conflicting national rules can increase costs, fragment services, and prompt market withdrawal by VPN providers.

Real-World Case Snapshots

- **India:** Customer-data retention requirements led several consumer VPN providers to withdraw physical servers from India, while continuing services through infrastructure abroad.
- **France:** Rightsholder litigation led courts to extend blocking duties to VPN providers, moving enforcement beyond Internet access providers.
- **Pakistan:** VPN registration evolved toward provider licensing. Iran and Russia illustrate restrictions on access to information and independent circumvention services.

What's Really Happening?

Governments are using retention rules, licensing, registration, blocking orders, distribution restrictions, and network filtering to pursue objectives ranging from public safety to censorship. Measures targeting a particular VPN provider's business practices can have different consequences from network-level blocking that affects multiple providers and lawful users.

Lessons Learned

Consumer and enterprise VPN deployments serve different needs but share foundational technologies; those differences alone do not establish a need for separate regulatory regimes. Network-level interventions may struggle to distinguish between them. A VPN protects a connection; it does not guarantee anonymity or prevent every cyberattack. Provider architecture, information collection and retention, jurisdiction, and governance shape a service's privacy and security protections.

Recommendations

- Target specific harms at the appropriate technical layer, using narrow, proportionate measures supported by reliable evidence of effectiveness.
- Direct obligations toward those who can reasonably identify and address the specific harm, taking account of their role and technical capabilities.
- Assess potential effects on lawful users, enterprise security, competition, and shared infrastructure.
- Strengthen VPN provider trust through data minimization, independent audits, transparency, and responsible governance.
- Include technical experts, industry, and civil society early in the consultation process; support international coordination and oversight.

Final Thought:

Effective policy must distinguish the conduct it seeks to address from the technology that enables secure communications. Protecting people and addressing legitimate harms require preserving the security infrastructure on which both individuals and organizations depend.