Psiphon was founded in 2006 out of the University of Toronto's Citizen Lab. Our goal is to provide access to online content and services for people living under censorship conditions worldwide.

Article 19

Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.
Psiphon’s Mission

Psiphon creates simple, easy to use tools that allow people all over the world to freely access open and unrestricted internet.

• Localized in over **40 languages including Persian, Arabic, and Mandarin.** We provide a single-click anti-censorship solution for all.

• Scale across devices and countries

• Continuous investment in research and development

• Extensive language support and community relationships
ACCESS THE ENTIRE INTERNET
Since 2006, Psiphon has provided open access to the internet for millions of citizens around the world.

Psiphon 2
https://583583.info/
Psiphon Apps

28 Million Users Worldwide

3.4 Million Users Worldwide

1 Million Users Worldwide
Psiphon client and server components implemented in Go. These components provide core tunnel functionality, handling all aspects of evading blocking and relaying traffic through Psiphon.

- `psiphon`
- `censorship-circumvention`
- `golang`

**Contributors:**
- `red-kynes`
- `psiphon`
- `vendor`
- `travis.yml`
- `CLA-entity.md`
- `CLA-Individual.md`
- `CONTRIBUTING.md`

**Commit Status:**
- `2,744 commits`
- `4 branches`
- `27 releases`
- `14 contributors`
- `GPL-3.0 license`
Censorship in Action

- IP Blocking
- DNS Hijacking
- Keyword Filtering
- Traffic Fingerprinting
- Next Gen. - National Intranets
Censorship in Action

Surf Safely!

This website is not accessible in Afghanistan

The Internet is a powerful medium for communication, sharing and serving our daily learning needs. However, the site you are trying to access contains content that is prohibited under the Internet Access Management Regulatory Policy of the Telecommunications Regulatory Authority of the Afghanistan.

If you believe the website you are trying to access does not contain any such context, please click here.

- IP Blocking
- DNS Hijacking
- Keyword Filtering
- Traffic Fingerprinting
- Next Gen. - National Intranets
Censorship in Action

- IP Blocking
- DNS Hijacking
- Keyword Filtering
- Traffic Fingerprinting
- Next Gen. - National Intranets
Censorship in Action

- IP Blocking
- DNS Hijacking
- Keyword Filtering
- Traffic Fingerprinting
- Next Gen. - National Intranets
Censorship in Action

- IP Blocking
- DNS Hijacking
- Keyword Filtering
- Traffic Fingerprinting
- Next Gen. - National Intranets
Censorship in Action

- IP Blocking
- DNS Hijacking
- Keyword Filtering
- Traffic Fingerprinting
- **Next Gen. - National Intranets**
How Psiphon Works

Psiphon deploys a number of circumvention protocols and traffic obfuscation methods to provide the most reliable anti-censorship service possible, regardless of location and observed method(s) of service interruption.

1. Open the app and click “Connect.”
2. The client app facilitates a geo-IP lookup, which allows Psiphon to generate a prioritized list of connection methods based on known regional network conditions.
3. Psiphon cycles through this list until a viable connection can be established.
4. The app displays a webpage, indicating you are successfully tunneled to the open Internet.
How Psiphon Works

User with Psiphon → Blocked Channel → Psiphon Network → Open Internet
Network Analytics

Tunnels connected by protocol

Bytes by protocol

Tunnel Establishment Duration

Tunnel Duration
Population-Scale Censorship

At the end of 2017, the Iranian government blocked Telegram, the most popular communication application in the country, and an estimated 40% of the country’s internet users began using the Psiphon network daily.
Population-Scale Censorship

At the end of 2017, the Iranian government blocked Telegram, the most popular communication application in the country, and an estimated 40% of the country’s internet users began using the Psiphon network daily.
Sudan Protests 2018-2019

- Widespread blocking of social media and messaging applications, and eventual mobile Internet blackout.
Sudan Protests 2018-2019

- Widespread blocking of social media and messaging applications, and eventual mobile Internet blackout.
Syria 2019

- The filtering of WhatsApp began throughout Syria in May 2018.
Psiphon Data Engine

The new public dashboard: psix.ca
Psiphon Data Engine

A data sharing and analytics platform for a more holistic understanding of the global censorship environment.
Psiphon Data Engine

The new public dashboard: psix.ca
Psiphon Data Engine

Forecasting and anomaly detection
Psiphon Data Engine

Join the PDE initiative: PDE@psiphon.ca
Thank You!

You can download Psiphon yourself from the App Store, the Google Play Store, or directly from our website: www.psiphon.ca

Work with us- drop me a line!

j.manco@psiphon.ca
Internet Censorship

Access series (Deibert et al.)