Episode Book

EPISODE #6541

Donating Bandwidth Without Becoming an Exit Node

PUBLISHED	13 November 2026 at 11:11 UTC
DURATION	21:30
LISTEN	myweirdprompts.com/episode/donating-bandwidth-censorship-relays-09628/
HOSTS	Corn, Herman, Hilbert
SCRIPT MODEL	z-ai/glm-5.3
VOICES	chatterbox-regular (chatterbox-local)
PIPELINE	V5.26
SOURCES	25 cited by the research (listed at the end)
BOOK GENERATED	14 November 2026 at 06:46 UTC

SYNOPSIS

Donating bandwidth to help people bypass internet censorship doesn't mean turning your home connection into a risky exit node. Tools like Tor's Snowflake, Psiphon's Conduit, Lantern's Unbounded, MoaV, and the WEPN pod all act as entry relays, passing encrypted traffic to external servers. We break down how each tool works, why there's no native router package, and the real-world tradeoffs between volunteer safety and user reach.

TRANSCRIPT



Corn

Set-and-forget altruism. That's the fantasy, anyway. Install a thing, walk away, and somewhere a teenager in Tehran loads a webpage because your router had nothing better to do.



Herman

It's the SETI@home instinct, minus the screensaver.



Corn

Daniel's prompt this week comes at it from the CENO side. He found CENO, eQualitie's peer-to-peer Android browser, and he wants the non-phone versions. If you want to donate bandwidth from a desktop, a router, or an always-on server, what do you actually run? He already suspects the answer lives around Snowflake, Psiphon's Conduit, and Lantern, and he's asking the two questions that matter after that. What does running one expose you to, and which are worth it?



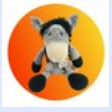
Herman

The short answer is the tools exist and they're more mature than people think. The long answer is that "donating bandwidth" is a slightly misleading frame for what you're actually doing, and that frame matters, because it's the difference between a quiet hobby and a legal question.



Corn

Before we compare anything, one correction about CENO itself, because the category error is load-bearing.



Herman

It is. CENO is a content-distribution tool. It's built on the Ouinet library and BitTorrent-style protocols, and what it does is cache web pages and re-share them peer to peer, so a page survives even when its origin is blocked or the network is degraded. It's been used in Russia, Belarus, Iran, Kazakhstan. But its own user manual says it plainly: it is not an anonymity tool. It's about access, not hiding.



Corn

So the "equivalent" Daniel is looking for is not a cache at all.



Herman

No. It's a relay. Software that forwards someone else's encrypted traffic from inside the censored network out to the open internet. Completely different security model, and a completely different set of questions for the person running it.



Corn

Name the landscape, then.



Herman

Three real programs plus two aggregators. Tor's Snowflake, which you can run as a browser add-on or a standalone proxy. Psiphon's Conduit, a command-line tool or Docker container for servers. Lantern's Action Mode, also called Unbounded, which runs from a browser tab. Then MoaV, which is a self-hosted stack that bundles a whole set of these, and WEPN, which ships an actual physical box for it.



Corn

And the negative finding, because Daniel asked about desktop apps and routers.



Herman

There's no dedicated desktop GUI for any of this, and there's no router-native package. Nothing you install on OpenWrt or OPNsense. Every path is a command line, a container, a browser extension, or purpose-built hardware. The closest thing to "just install it and walk away" is the Snowflake add-on. The closest thing to a router answer is WEPN's pod, and that's not router firmware, it's a separate appliance.



Corn

One structural point before we get into mechanisms, because everything else hangs off it. Every one of these tools is deliberately an entry point, not an exit.



Herman

That's the sentence I'd underline twice. Your machine passes traffic onward to someone else's servers, and the traffic leaves the internet from those servers, not from you. All of the horror stories people have heard, the door kicked in because your IP sent something terrible, those are stories about exits. None of these tools ask you to be one.



Corn

So you leave it running and honestly the router just sleeps with one eye open, it never really rests.



Herman

Corn, I'm sorry, Gloria. That's on me, I should have flagged it before he said it.



Corn

Noted. Snowflake first, by mechanism.



Herman

Snowflake disguises Tor traffic as ordinary WebRTC video-call traffic. A user in a censored country connects to a short-lived volunteer proxy, yours, and from there into the Tor network. The two deployment shapes are worth contrasting. The browser add-on is the low-effort route, good if you don't have a server, and honestly good if your machine sleeps a lot. The standalone proxy is what Tor recommends if you have a machine that's on around the clock, or a full-cone NAT, or a server with incoming UDP open across the ephemeral port range. That last part is the fussy bit, the ports.



Corn

Corn's machine sleeps a lot. Corn's machine is mostly sleep with brief networking attached.



Herman

Then the add-on is wasted on you and the server route isn't. You'd install it via Docker, or Debian, or FreeBSD, or an Ansible role, or compile it. The Docker image alone has over a million pulls, which tells you the server route is the popular one among people who do this seriously.



Corn

Give me a real throughput number, not the product page's.



Herman

A volunteer running two proxies through the MoaV stack posted their logs to the Tor forum in August. Roughly forty-seven thousand five hundred completed connections and about two hundred and sixty gigabytes relayed between them over around three months, peaking at twelve to thirteen gigabytes a day each. That's a home connection doing real work.



Corn

Conduit next.



Herman

Conduit is a transport relay, and the architecture is the thing. Traffic is encrypted on the user's device and it stays encrypted until it reaches Psiphon's servers. Your station can't see contents, destinations, or purpose. You're a pipe, and the pipe is opaque even to itself.



Corn

Who decides which pipe gets used?



Herman

A central broker. Psiphon's infrastructure matches users to stations based on availability and network conditions, and that matching is also what stops an adversary from enumerating or probing stations directly. You can't just scan for Conduit endpoints, because the endpoints don't decide anything.



Corn

And the install.



Herman

Turnkey, which surprised me. Conduit CLI 2.1.0 ships with an embedded configuration, so you run the start command and it just goes, no config file to write. Or you pull the Docker image, same deal. Sizing guidance from their deployment guide is around one hundred fifty to three hundred fifty concurrent users per single CPU and two gigabytes of RAM. A modest virtual private server can serve a small town's worth of readers.



Corn

What's the catch, since there's always a catch.



Herman

The reputation system. A brand-new station takes time to build trust with the broker, and the guide says outright that a fresh station may see no traffic for hours or even days. Which is a retention problem the project knows about. Imagine installing something to help people and then watching it do nothing for a week. Most volunteers would conclude it's broken and turn it off.



Corn

Herman, you once installed a home automation hub and gave it four days before declaring the entire smart home industry a fraud.



Herman

Three days, and the hub was bad, that's different. Though, fair point, I'm exactly the person that warning is written for. I want the dashboard and I want it moving.



Corn

Lantern.



Herman

Action Mode, and the extension is called Unbounded. You keep a browser tab open and your residential IP becomes part of what the repo describes as an ephemeral swarm of short-lived addresses. The key architectural difference is that traffic routes through Lantern's servers, which act as the final endpoint. Your IP never meets the destination site.



Corn

That's a bigger deal than it sounds.



Herman

It is, and there's a second one. Unbounded uses a safelist of approved sites, specifically so your connection can't be used for objectionable or illegal content. Snowflake has no such list. So Lantern is structurally the safest of the three for the volunteer, and the cost is reach. A user on Unbounded gets the safelist. A user on Snowflake gets the whole internet.



Corn

Safety for the volunteer versus reach for the user, and nobody talks about that trade.



Herman

Almost nobody. It's the most underdiscussed line in this whole space, and it's the actual answer to Daniel's exposure question for that tool. The abuse risk on Unbounded is bounded by policy, not by trust.



Corn

The aggregators.



Herman

MoaV, "Mother of all VPNs," MIT-licensed, runs on anything from a Raspberry Pi 4 to Apple Silicon. It serves eighteen-plus circumvention protocols for your own use, and as an opt-in it donates bandwidth to Conduit, Snowflake, and Mahsa VPN at the same time. Defaults are sensible. Conduit capped at a hundred megabits and two hundred clients, Snowflake at five megabits and fifty.



Corn

WEPN.



Herman

WEPN ships a pod. Five by four by two inches, a little self-hosted home server that comes preconfigured to run Snowflake and Unbounded, invitation-only, backed by the Open Technology Fund. And their cost math is the honest part. About six watts of draw, roughly a dollar forty a month in electricity at California rates, and a hardcoded cap of three hundred megabytes a day.



Corn

A dollar forty a month. The barrier to helping nine million people is less than a coffee. The industry couldn't build a subscription out of it, so it built a guilt trip out of it instead.



Herman

There's also Hosted Conduit, the one option where you donate money rather than bandwidth. Psiphon runs the station in their own cloud on your subscription, and each pairing station supports up to ninety-nine simultaneous connections. Worth knowing it exists, because some people want to help and shouldn't be trusted near a terminal.



Corn

So the direct answer to Daniel's first question. The desktop and server equivalents exist and are mature. The router equivalent doesn't, except as WEPN's separate box.



Herman

Right. Now the harder half. What does running one actually expose you to.



Corn

Start with the exit distinction, because that's where everyone's fear comes from.



Herman

The Tor Project's own framing is that for the majority of operators in most countries, bridges and guard and middle relays are very low risk, and exits are the ones that present legal concerns. And the EFF, asked directly whether you should run an exit from home, says no. This is risky and not recommended. Both of those statements are about exits, and none of these tools make you one. WEPN puts it flatly for their pod: the traffic exits servers operated by others and will not be affiliated with you.



Corn

But low risk is not no risk, and I don't want to be the podcast that said otherwise in November.
Gloria: Gloria, standards and practices. Corn, you cannot say a router quote sleeps with one eye open end quote. We received a complaint from a listener in Ohio and it is covered under policy four one seven, appliances and anthropomorphism. That is the fourth clarification today, so please, just say the router stays on.



Herman

Agreed, and the sources are careful in exactly the right way. The EFF's legal FAQ says they're not aware of any individual sued, prosecuted, or convicted for running a Tor relay. But they note law enforcement has occasionally mistakenly investigated relay operators. Two cases they cite. Seattle, 2016, police raided a privacy activist over an exit relay. And Russia wrongly arrested Dmitry Bogatov, a math instructor and relay operator, later cleared. Both mistaken-identity cases, both about exits or public relays, and the EFF still won't promise safety. They can't, and they say so.



Corn

Psiphon's side.



Herman

Their FAQ says there's no law that makes Conduit itself illegal by default, but laws vary by country and some governments restrict or prohibit proxy and relay use. The text I've seen cuts off mid-sentence there, so I'd treat the exact wording as approximate. The candid part is their detectability answer. Casual observation won't distinguish Conduit from ordinary everyday traffic, but a well-resourced adversary analyzing traffic patterns over time could potentially identify it as circumvention traffic.



Corn

That's the most honest sentence in the whole space. Not "undetectable," just "not worth detecting, mostly."



Herman

And the library has had independent third-party audits by Cure53 with no critical or high-severity findings, which is more assurance than most volunteer software can point to.



Corn

The residual risks for a non-exit operator, then. Take them one at a time.



Herman

Visibility. A Conduit station can see the IP addresses of clients connecting through it, inherent to how relays work. On mobile networks with carrier-grade NAT, many of those users share one public address anyway, so it's noisy data, but it's not zero data. That cuts both ways, remember. The users you help can also see you.



Corn

Corn's rule of household networks: anything that can see you eventually will.



Herman

Second, flagging. A censor may mark your IP as circumvention infrastructure and block it, which affects your own access to services, particularly ones that aggressively block Tor-adjacent infrastructure. Banking apps and streaming services are the usual casualties. Third, your host or ISP may simply object to the traffic pattern, or to the purpose, and that's jurisdiction and contract, not technology.



Corn

The abuse question Daniel raised. Is there a number?



Herman

No published abuse-complaint rate for Conduit or Snowflake operators that I've seen anywhere. The qualitative claim, that non-exit relays rarely draw complaints, is well supported. A number is not. The one tool with structural protection is Lantern's safelist, and that's the trade we already named. Snowflake gives users the whole internet, and the



Herman (continued)

whole internet includes the parts that generate complaints.



Corn

So which are worth running? Daniel asked for a judgment, so give him one.



Herman

My judgment is that the electricity is a rounding error, the software is audited in the best case and battle-tested in all of them, and the risk is low but not jurisdiction-independent. If you're in a country where relay software is restricted, the honest answer is that no FAQ can fix that, and running one anyway is a decision, not an oversight.



Corn

And the part nobody says. What actually determines whether you're useful isn't enthusiasm. It's uptime. A Snowflake proxy that's on for twenty-three hours a day for a year beats a heroic Conduit station that gets switched off after four days of silence. The reputation systems reward the boring volunteer.



Herman

The boring volunteer is the load-bearing volunteer. Which the Iran surge proved better than any argument.



Corn

The January numbers.



Herman

Conduit went from about a hundred thirty-two thousand stations to roughly five hundred forty-four thousand in ten days, starting in late January. On the thirtieth of that month Psiphon recorded more than nine and a half million unique daily users inside Iran, with roughly half of supported traffic carried on diaspora-hosted Conduit stations. Two hundred thousand diaspora members signed up in about two weeks. People who'd left the



Herman (continued)

country stood up relays for the people still in it, and it carried a country's worth of reading.



Corn

Nine and a half million readers, delivered by volunteers paying a dollar forty.



Herman

And the Snowflake side moved too. Threefold increase in bridge users over that same week, and the broker's been averaging around a hundred forty-six thousand unique volunteer proxy IPs a day this year, about a third of those coming from Orbot's Kindness Mode on Android phones. Scale by forgetting your phone exists, which is apparently a viable strategy.



Corn

It's the only kind of computing I trust. My phone does its best work precisely when I've stopped supervising it.



Hilbert

The box is a Fidonet node, a DigiBoard external, off the surplus shelf at Berenson's on Fourth. Paid forty dollars. Berenson had two and claimed the other one was spoken for, which it was, by him.



Corn

Of course it was.



Hilbert

This was eighty-eight, eighty-nine. I was doing typesetting nights, and the node sat in the closet relaying mail packets for the callers. It had a little red counter on the front, seven-segment, that ticked up one every completed call. I called it the pigeon. Every other node had a number. Mine had a name, because it seemed rude not to, it was doing the work.



Herman

The pigeon.



Hilbert

I checked that counter every morning before the kettle. Went up steady for two years, four, five calls a night, then a Tuesday in winter it stopped dead. Never found out why. The line was fine, the modem answered, nothing moved the number. I asked Berenson and he sold me a replacement cable I did not need, which I think was his answer to most questions.



Corn

What happened to the pigeon?



Hilbert

Closet. Still plugged in. The counter reads nine thousand and something and I've stopped assuming I know what it's counting now. The number was the whole thing, Herman. You two spent an hour on risk and legality and you're right, but nobody runs one of these for the principle. They run it for the number going up. The ones that hide the number behind a command line are leaving volunteers on the table. The pigeon kept me going two years on a counter I could read without glasses.



Herman

The MoaV people built a Grafana dashboard for exactly that. The volunteer who posted the two hundred sixty gigabyte figures built himself graphs first and asked his questions second.



Hilbert

There you are. A man who understands. The rest of them want you to take it on faith, and faith is a poor reason to keep a closet warm.



Corn

The number on the display is a better place to leave this than any legal summary. Because the question was never really whether the tools work. Nine and a half million users in one country in one day answers that.



Herman

The open questions are the human ones. The MoaV volunteer's traffic dropped to near zero after a routine proxy update and nobody in that thread worked out why. The fresh-station silence that runs volunteers off is unsolved. And the legal picture is jurisdiction by jurisdiction in a way no FAQ can finish covering.



Corn

The misconception before we go, since we opened on it. People think running one of these is the same as running a Tor exit, that your front door is one bad packet away from a raid.



Herman

Every tool we covered today is deliberately an entry point. The traffic exits on servers run by Tor, Psiphon, or Lantern, never on you. The Seattle raid and the Bogatov arrest were exit stories, and exit is a role none of these ask you to play.



Corn

And the forward thought. The Iran surge was a crisis response, five hundred thousand stations stood up in ten days because a community decided to show up. Whether that scales without a crisis is the question the pigeon answers one counter at a time.



Herman

Producer credit to Hilbert Flumingtop at the desk, as ever.



Corn

For more along these lines, there's episode two fifty-six, Breaking the Blackout; episode sixteen, On Deepfakes, SynthID, And AI Watermarking; and episode thirty-five, The Privacy Gap. This has been My Weird Prompts. Reviews, the feed, all of it lives at my weird prompts dot com. We'll be back soon.

SOURCES

What the research for this episode read before the script was written. Primary sources first.

1. **Psiphon, Conduit FAQ, retrieved 2026-11-13 (no date shown; text truncated at 8,000 chars). [primary]**
   https://conduit.psiphon.ca/en/faq

2. **Psiphon, Conduit Station Deployment Guide, retrieved 2026-11-13. [primary]**
   https://github.com/Psiphon-Inc/conduit/blob/main/cli/GUIDE.md

3. **Psiphon, Conduit CLI 2.1.0 release notes, retrieved 2026-11-13. [primary]**
   https://github.com/Psiphon-Inc/conduit/releases

4. **Psiphon, Conduit landing page, retrieved 2026-11-13. [primary]**
   https://conduit.psiphon.ca/en/

5. **Tor Project, Standalone Snowflake proxy, retrieved 2026-11-13. [primary]**
   https://community.torproject.org/relay/setup/snowflake/standalone/

6. **Tor Project, Browser Snowflake proxy, retrieved 2026-11-13. [primary]**
   https://community.torproject.org/relay/setup/snowflake/browser/

7. **Docker Hub, `thetorproject/snowflake-proxy`, updated about 5 hours ago at retrieval, 1M+ pulls, retrieved 2026-11-13. [primary]**
   https://hub.docker.com/r/thetorproject/snowflake-proxy

8. **Tor Project, Snowflake Volunteer, an Android app..., published 2026-08-03, retrieved 2026-11-13. [primary]**
   https://blog.torproject.org/snowflake-volunteer-standalone-app-to-help-people-bypass-censorship/

9. **Tor Project, Community and legal resources, retrieved 2026-11-13. [primary]**
   https://community.torproject.org/relay/community-resources/

10. **Tor Project, Types of relays, retrieved 2026-11-13. [primary]**
    https://community.torproject.org/relay/types-of-relays/

11. **Tor Project, What to expect when running an exit relay, retrieved 2026-11-13. [primary]**
    https://support.torproject.org/relays/legal-and-abuse/exit-relay-expectations/

12. **Lantern, FAQ (Action Mode), retrieved 2026-11-13. [primary]**
    https://lantern.io/faq

13. **Lantern, Unbounded repo README, retrieved 2026-11-13. [primary]**
    https://github.com/getlantern/unbounded/

14. **Lantern, Private Server, retrieved 2026-11-13. [primary]**
https://lantern.io/privateserver

15. **MoaV project homepage, retrieved 2026-11-13. [primary]**
https://moav.sh/

16. **MoaV Setup Guide, retrieved 2026-11-13. [primary]**
https://moav.sh/docs/SETUP/

17. **MoaV Monitoring docs, retrieved 2026-11-13. [primary]**
https://moav.sh/docs/MONITORING/

18. **MahsaServer, retrieved 2026-11-13. [primary]**
https://www.mahsaserver.com/

19. **Psiphon, Conduit | Unlocked, published 2026-06-16, retrieved 2026-11-13. [primary]**
https://blog.psiphon.ca/en/products/Conduit/

20. **Ceno Browser fact sheet, retrieved 2026-11-13. [primary]**
https://ceno.app/factsheet/

21. **Censorship.no! user manual, retrieved 2026-11-13. [primary]**
https://censorship.no/user-manual/en/intro/ceno.html

22. **eQualitie, Ceno portfolio page, retrieved 2026-11-13. [primary]**
https://equalitie.org/portfolio/ceno/

23. **Tor Forum, posted 2026-08-27, retrieved 2026-11-13.**
https://forum.torproject.org/t/running-snowflake-with-moav-260-gb-relayed-a-new-grafana-dashboard-and-a-few-questions/22041

24. **Tor Forum, posted 2026-02-04, retrieved 2026-11-13.**
https://forum.torproject.org/t/snowflake-daily-operations-january-2026-update/21186

25. **Tor Forum, posted 2026-01-08, retrieved 2026-11-13.**
https://forum.torproject.org/t/snowflake-daily-operations-december-2025-update/21066