Episode Book

EPISODE #6576

What It Actually Costs to Run an Anonymous Tip Line

PUBLISHED	13 November 2026 at 21:58 UTC
DURATION	22:11
LISTEN	myweirdprompts.com/episode/self-hosted-anonymous-tip-lines-24251/
HOSTS	Corn, Herman, Larry, Hilbert
SCRIPT MODEL	z-ai/glm-5.3
VOICES	chatterbox-regular (chatterbox-local)
PIPELINE	V5.26
BOOK GENERATED	14 November 2026 at 06:47 UTC

SYNOPSIS

Running an anonymous tip line without institutional backing comes down to custody, maintenance, and whether sources can even reach you. A real-world ledger compares SecureDrop, GlobaLeaks, Hush Line, OnionShare, Signal usernames, and raw Tor onion services—from SecureDrop's multi-thousand-dollar hardware list to GlobaLeaks' modest specs and Hush Line's hosted-first approach. It also examines why Tor bridges like Snowflake and WebTunnel matter more than onion addresses in censored countries.

TRANSCRIPT



Corn

Why would a small newsroom want to run its own anonymous tip line? Daniel asks that question in a way that answers half of it, because he knows how it sounds — "why would you want to run your own anonymous tip line?" — like the answer involves a filing cabinet and a burner phone. His argument is that the reasons are ordinary: custody, jurisdiction, cost, not being somebody's customer, and in censored places, being reachable at all.



Herman

This is part three of the whistleblowing series, and it's the one where the camera flips around. Part one was the usability problem, part two was the tools the big institutions get handed — and today is the version where you're a freelance journalist, an NGO, an activist group, or a podcast with no institution behind you, and the question is what you can actually run yourself.



Corn

Right, and he wants the real ledger, not vibes — what SecureDrop, GlobaLeaks, Hush Line, OnionShare, Signal usernames and raw onion services each cost in money and in maintenance, who each one is for. And then the case study he volunteered us for: our own tip line, and why we chose hosted Hush Line instead of putting a server in the flat.



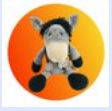
Herman

I want to be clear that I looked at the SecureDrop hardware list again before this episode, purely for the pleasure of it.



Corn

Purely for pleasure. That's the most Herman sentence ever recorded.



Herman

It's a beautiful bill of materials! Two dedicated NUC-class servers, each with two two-hundred-and-forty-gigabyte SSDs and sixteen gigs of RAM. A dedicated physical firewall with four network ports. One or two Qubes-compatible laptops with thirty-two gigs of RAM. USB drives. An optional offline printer. The docs put the recommended hardware total at around two thousand two hundred to two thousand four hundred dollars, and then



Herman (continued)

the planning section says normally two to three thousand.



Corn

Two different numbers in the same documentation for the same shopping list.



Herman

I actually find that reassuring. It means the number is being written by people doing the work rather than people doing the marketing. Though your face suggests you read it differently.



Corn

My face is doing arithmetic. That's a used car that only sends and receives ciphertext. And the money isn't even the barrier, is it.



Herman

No, and this is the part that gets glossed over. The admin has to be comfortable with Linux and Bash. Setup takes at least a day, with a full week recommended for setting up and testing. Staff training is half a day just to introduce the thing and at least a full day to reach proficiency. They recommend backup admins — plural, people, backup admins — and the organisation has to own the hardware and keep it on its own premises. That's not an app you install. That's a small department.



Corn

The design is the tell. Two servers, a firewall, an air-gapped viewing station for opening documents. It's a rule about custody expressed in hardware.



Herman

And the workstation side is in flux right now — the current docs describe moving the journalists' workstations to Qubes OS, while the older stable page still describes Tails for the journalist workstation plus an air-gapped Secure Viewing Station. I wouldn't quote



Herman (continued)

either arrangement as settled. What is settled is that the Freedom of the Press Foundation will do pro-bono setup and training for smaller news organisations, and honestly that's the realistic on-ramp. A four-person newsroom that needs SecureDrop-grade assurance should be talking to them, not reading the hardware page alone at midnight.



Corn

Which they will anyway.



Herman

Which they will anyway, and then they'll find GlobaLeaks and calm down.



Corn

GlobaLeaks is the rung I'd assumed everyone like us would land on.



Herman

It's a real step down in machinery but not a fake one. Requirements are a dual-core two-gigahertz CPU, one gigabyte of RAM, twenty gigs of storage. That is a computer you already own or can find in a cupboard. It runs on Debian and Ubuntu only — Debian thirteen and Ubuntu twenty-four-oh-four recommended — installed through a script from the project's own package repository, checksum provided, or via Docker if you like. And what you get for that is surprisingly institutional: automatic Let's Encrypt certificates, automatic Tor version-three onion service setup, updates through a Debian package repository, and multi-site support, so if you're a small collective running tips for three different projects, they can live as virtual sites on one install.



Corn

The governance on it is worth stating plainly, because it changes what maintenance means.



Herman

It's AGPLv3 with additional terms allowed under section seven, developed by the Hermes Center for Transparency and Digital Human Rights, community-driven, no major corporate backer, donations through GitHub Sponsors. Latest release is 5.0.101, end of October. So the bus factor is real — a small team's pace, not a product roadmap — and "who patches this when the people doing it move on" is part of the honest cost.



Corn

There's a limit in the docs I want held up to the light, because it busts the biggest misconception in this whole space.



Herman

The docs say, fairly plainly, that hiding the server's own location or the administrator's identity requires advanced procedures beyond the simple install guide. So the easy install gives you a working tip line, not an untraceable one. The encryption protecting messages is real from the start. But if your threat model is "the hosting provider or an observer learns where this box is," you're past the install guide.



Corn

"Self-deployed" has a lying module built into the phrase. It implies the anonymity comes free with the SSH session.

L

Larry

Friends, you have been hearing about self-deployed tip lines all episode, and I have been hearing one question on your lips: Larry, how do I make my own anonymous channel feel like a premium monthly treat? Introducing the Tip Line Crate, a subscription box that arrives every month with a fresh, artisanal tip inside it. Choose your tier. The Copper Whistle gives you one tip, unwrapped, and a small hat. The Gold Whistle gives you two tips, both written in pencil by a stranger we have never met, plus a card explaining jurisdiction. And the Platinum Dead Drop, our most popular tier, delivers a fully self-deployed onion service straight to your door in a handsome wooden crate, no hardware required, no maintenance, no admin, no Tor, because we handle all of that, and also none of it. Cancel any time, by which we mean never, and if you do cancel we will publish your name, your address, and your favourite podcast. Tip Line Crate. Tip lines, but a crate.



Corn

Right. Hush Line, the one we actually run.



Herman

Made by Science and Design, a US 501(c)(3) nonprofit, AGPL-3.0, and the version number is the thing I keep pointing at: the latest release is v0.7.36, early November. Pre-1.0. That's not a knock — it's a signal about maturity that a small org should walk in knowing. The flagship is the hosted service at tips.hushline.app, a managed thing: free core tier with verified accounts, end-to-end encryption, email forwarding and a Tor onion service, paid tiers for small businesses and a dedicated single-tenant option, pricing marked subject to change, so I won't quote numbers.



Corn

The crypto matters more than the tier names, because it's what makes the hosted-versus-self-deployed comparison honest.



Herman

Messages are encrypted in the sender's browser using OpenPGP.js to the recipient's PGP key, with a server-side fallback path if the browser can't do it — which is itself a trade-off worth knowing about. The tip page tells users to run Tor Browser and shows the onion address. There are Subgraph audits listed for 2024 and a preliminary one for 2025. So it's an audited, small, checkable operation — which is exactly the shape of thing I trust more than a big company's self-reported retention schedule.



Corn

Then the self-hosted route, which is where the documentation gets thin.



Herman

Thin. The Hush Line Personal Server is described as an appliance: a Tor onion address for sources, a local-network HTTPS address for administration, first registered user becomes admin, and the docs say to publish the onion address. What the docs don't name is the hardware. The Science and Design shop lists a device at five hundred dollars described as Tor-only, availability unclear. Their tutorial from a couple of years back installs Hush Line on a Raspberry Pi 3 B+, with a Pi 4 or a VPS as alternatives. So a Pi self-install is documented — but what's actually inside the shipped Personal Server, I can't confirm, and



Herman (continued)

the production self-hosting quickstart is a local Docker setup. It reads like a project whose energy goes into the hosted service first.



Corn

Which is itself an answer to who it's for. Now the light end, and I want the "what each is not" said cleanly.



Herman

OnionShare receive mode, latest 2.7.2, published just this month — it turns your own computer into an anonymous dropbox on a temporary onion address. Senders need Tor Browser. The address disappears when you stop or suspend the machine. The docs recommend a dedicated always-on computer if you're serious, it does not scan files for malware, and the address and key have to be shared securely in the first place. For a one-off, or a drop for a small known audience, it's excellent. As a public standing tip line, it's a drawer you keep in your pocket.



Corn

Signal usernames.



Herman

Launched February 2024. They let people contact you without learning your phone number, and there's a setting so only someone with your exact username can start a chat. But you still need a phone number to register the account, so it's a secondary contact route, not an anonymous drop. Our own tip-line page suggests it as an optional encrypted reply contact, which is the correct job for it. And raw Tor onion services are just the substrate everything here sits on — an onion service is plumbing, not a product. You can hand-roll one, and a serious self-deployer eventually will, but at that point you're the developer.



Corn

So that's the ledger. But cost isn't the only thing that decides whether a tip line works, because a tip line that can't be reached isn't a tip line.



Herman

And this is where Daniel's censorship point earns its place. The reasoning goes like this: an onion service protects the source from exit-node snooping and from domain-level blocking of your address. But the source still has to reach the Tor network first. So in a censored country, bridges come before onions — every time. Meanwhile a plain HTTPS tip line may work fine where Tor is blocked, but it can be blocked by domain, and then it's gone. Running your own means you can offer both doors and rotate addresses when one gets slammed. That flexibility — not anonymity per se — is the actual product of self-deployment.



Corn

Paint the current picture, because it's moving fast.



Herman

Iran first. Per the Tor Project's own write-up on staying ahead of censors, Snowflake is the most-used circumvention tool there, in a country where internet access was cut outright for days in June 2025. Conjure, which hides traffic in unused address space inside cooperating ISP networks, was planned for rollout. Russia: allowlist-based blocking and address-block censorship have grown, WebTunnel became a key tool because it blends into ordinary web traffic, and in June 2025 the censors began listing most WebTunnel bridges — so Tor moved WebTunnel into its Telegram bridge distributor. Ordinary people run Snowflake proxies from a browser extension, which is one of the quietest useful volunteer jobs on the internet.



Corn

The numbers on scale.



Herman

Tor's own metrics, medium confidence on this, put it around three point two million direct users a day and about two hundred twenty-five thousand bridge users, averaged over the month into early October. What's grim is the 2026 texture: forum and mailing-list reports from Iranian users saying no bridges worked at all, and Russian stretches where only allowlisted domestic services are reachable and Tor is unusable for hours at a time. Reachability is a moving target, and if you self-deploy, the person who has to keep re-hitting it is you.



Corn

Which leads us to the smallest possible version of this decision. Ours.



Herman

The tip line lives at the hosted Hush Line address under the account "mwp". The short link, my weird prompts dot com slash anon-prompt, redirects there, and there's an explainer page at slash tipline. The PGP key is an ed25519 key with a cv25519 encryption subkey, created this month, expiring November 2029, and the fingerprint is published in three places — our own page, the Hush Line profile, and the key file itself — so a listener can match all three and know the key they're encrypting to is ours and not someone else's.



Corn

Walk the flow, because the flow is the whole argument.



Herman

The sender's browser encrypts the message to our public key before anything leaves their machine. Hush Line stores and forwards only ciphertext. It arrives to us as an encrypted email that only our private key can open. Our own website handles none of the submissions — it just points at the door. And I'll note honestly: a page fetch didn't show a verification badge on the Hush Line profile, so I won't claim one.



Corn

Now the trade, stated plainly, because I'm the one in the flat who'd be doing the maintaining.



Herman

You would. And the show is tiny — we expect a handful of messages, mostly sensitive personal questions, not leaked documents. Self-deploying would add a server to patch, an onion service to keep up, and a mail path to run, for the same core security property. Because that's the thing: encryption to a key only we hold is true either way. The browser encrypts to our key whether the box serving the page is in the flat or in a data centre. What we give up by hosting is a third party's availability, the metadata it can see, and reachability tied to its domain. That's the whole trade. At our scale it's obviously right, and for a newsroom handling leaked documents it's obviously wrong.



Corn

I'd put one disagreement on the table, though, because the folklore version of this is "self-deployed is always more private."



Herman

And I'd push back on the folklore. A badly run self-deployed server can be worse than a well-run hosted one — an unpatched box, a leaked admin identity, an onion service that's been down for three weeks and nobody noticed, sources trusting a door that opens onto a cupboard. The custody is only better than the service if the custodian is awake.



Corn

I resemble that. I am mostly asleep, and I know it.



Herman

We all know it.



Corn

So the decision rule, without turning it into a checklist: it's not "how secure is each option," it's three questions. What's the sensitivity of what you expect to receive? What's your actual maintenance capacity — not your enthusiasm this week, your capacity in February? And what does your threat model say about who can compel or observe the custodian? SecureDrop for document leaks with institutional backing, ideally with the Foundation's pro-bono help. GlobaLeaks for a small org that wants its own server and will patch it. Hosted Hush Line for a tiny operation whose core need is encrypted contact. OnionShare for a one-off. Signal username as a second door, never the drop.



Herman

And notice what decides most of those — not the cryptography, which is roughly table stakes across the board, but who's on call when the address stops working.



Hilbert

Corn, can I ask you something. When you set up your tip line, did you print the address or send it?



Corn

The link's on the site. Sent, in effect.



Hilbert

I don't send mine. I keep the onion address on a card in my wallet and read it out to people, because I don't trust that a sent address hasn't been copied somewhere on the way. I've run my own line for some years now. Same address the whole time. I've given it to maybe five people, and I read it to each of them off the card. It's never changed and I've never had to read it out in a hurry, but the card's in the wallet anyway.



Herman

You've been running an onion service the whole time we've been recording these.



Hilbert

I agree with the two of you about hosted versus self-deployed, but you've undersold the maintenance, Herman, and you were the one going on about backup admins. My arrangement has a rule that I restart the thing every Sunday whether it needs it or not. I have never once been sure that was necessary. I keep a written log of every time the line has been down. The log has one entry in it. A power cut, 2019, four hours. I kept the notebook.



Corn

One entry. In a notebook.



Hilbert

The notebook was already there. I'm not buying a second one.



Corn

A log with one entry is either a very good tip line or a very patient man.



Herman

The Sunday restart is the part I recognise — that's exactly the FPF's week-to-set-up instinct compressed into one man. You're the backup admin, Hilbert. You're the whole admin.



Hilbert

Somebody has to be. Herman, you said the address disappearing was OnionShare's problem. It's everybody's problem. That's the log.



Corn

The card in the wallet — that's reachability in its smallest form. The address lives where the censor can't reach it because nobody's routing it anywhere.



Herman

Though I notice he trusts a piece of cardstock more than a TLS handshake.



Corn

Cutting-room floor before we go. The detail I couldn't fit earlier: the Hush Line repository also ships tooling to sync a public directory of tip lines — GlobaLeaks and SecureDrop instances included. A directory of live drop boxes that updates itself is its own quiet infrastructure, and it exists mostly unnoticed inside a GitHub repo.



Herman

And Conjure, from the Tor write-up — parking traffic in unused ISP address space — is the one I'd watch. If that scales, the arms race changes shape again, and every tip line's reachability question changes with it.



Corn

The question I'd leave hanging: as hosted tip-line services mature and self-hosting docs stay thin, the small-org default quietly becomes renting from a nonprofit — and a source trusting that custodian is trusting a third party nobody at the organisation has ever met. Whether that trust is something you earn with a fingerprint and three published copies, or something you can't earn at all, is the part I'm still turning over.