Episode Book

EPISODE #6577

How SecureDrop and GlobaLeaks Run in Practice

PUBLISHED	13 November 2026 at 21:59 UTC
DURATION	26:19
LISTEN	myweirdprompts.com/episode/institution-grade-whistleblowing-systems-25427/
HOSTS	Corn, Herman, 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

Whistleblowing systems rarely fail on cryptography—they fail operationally. An audit of institution-grade tooling reveals that the real divide isn't open-source versus commercial, but supplied-and-supported versus self-deployed. The episode examines SecureDrop's two-server architecture and its transition to isolated Qubes OS workstations, alongside GlobaLeaks's dual Tor and HTTPS model for public authorities like Italy's ANAC. It also compares these open-source platforms with commercial SaaS tools like EQS Integrity Line, NAVEX, Whispli, and Vault.

TRANSCRIPT



Corn

The romantic version of whistleblowing is a man in a raincoat meeting a reporter under a bridge. The actual version, mostly, is a form on an onion address and a case management system with a feedback deadline.



Herman

And someone has to run all of that.



Corn

That's where Daniel went. He's been looking at how whistleblowing actually reaches institutions, and he wants an audit of the tooling the serious players rely on, the systems that are supplied to them and supported for them rather than cobbled together. SecureDrop on the open-source side, GlobaLeaks for NGOs and public authorities, and the commercial platforms companies buy since the EU Whistleblower Directive made internal channels mandatory. His line, which I like, is that he doesn't want the commercial ones framed as the real stuff with open source as the poor cousin. He says the real distinction is institutional, supplied-and-supported versus self-deployed.



Herman

Which is the right cut, and it's not the one most coverage makes. Before we can say what these systems do well, we need to be precise about what institution-grade actually means here, because the obvious split, open-source versus commercial, is not the one that matters.



Corn

Say it plainly, then.



Herman

A newsroom running SecureDrop with a priority support contract, vendor-trained admins, a maintenance schedule, that's in the same institutional category as a company buying EQS Integrity Line. Both have an organisation standing behind the tool. A GlobaLeaks instance someone in the IT department set up to tick a box and then left to rot, that's a different category entirely, even though the software is identical to the one ANAC runs.



Corn

And the reason the category matters is that whistleblowing systems almost never fail on the cryptography.



Herman

Almost never, no. They fail operationally. An unmaintained server, an admin who never rotated a key, a channel nobody monitors, a reporter who didn't know the deadline. Supplied-and-supported is buying operational competence as much as software.



Corn

Give me a failure that isn't cryptographic, so listeners can picture it.



Herman

The pattern is an inbox that works perfectly and is checked quarterly. The submission arrives encrypted, sits encrypted, and the source waits. Or the admin leaves and nobody else holds the keys. The maths holds up beautifully in cases like those. The institution doesn't.



Corn

Three families on the table, then. SecureDrop, the newsroom model. GlobaLeaks, the NGO and public-authority model. And the commercial platforms, EQS, NAVEX, Whispli, Vault, which exist in their current form largely because a directive in Brussels told fifty-person companies they had to have a channel.



Herman

Let's do them in order of how paranoid they are.



Corn

SecureDrop wins that before the race starts.



Herman

SecureDrop is the clearest example of institution-grade design, so start with the architecture, because the architecture is the argument. Two physical servers, in the news organisation's own hands, on private servers it controls. Not rented cloud. The Application Server runs Ubuntu and hosts two Tor onion services. One is the public Source Interface, that's the page a whistleblower reaches through Tor Browser. The other is the authenticated Journalist Interface, where reporters log in, also over Tor, also an onion address.



Corn

Two onions on one box.



Herman

Right, and the second physical machine is the Monitor Server. It watches the Application Server with OSSEC, an open-source host intrusion detection system, and it emails alerts. The whole point of the separation is that the monitor is the tripwire. You design on the assumption that the Application Server will eventually be compromised, and you want a second machine watching it, so you find out.



Corn

The assumption being that the thing you protect will fall, so you build the thing that notices.



Herman

That's more elegant than how the docs put it, but yes.



Corn

Why the insistence on premises, though? A cloud instance is still your instance, your keys, your login.



Herman

Because with rented cloud you're trusting the hypervisor, the provider's staff, the provider's government, and every other tenant on the machine. Premises doesn't remove trust, it concentrates it in people you can walk over to and shout at. For a newsroom whose adversary might be a state, that's the trade they make. It's not that cloud is impossible to secure, it's that the threat model makes premises the cheaper assumption.



Corn

Then the interesting part, what happens after the leak lands.



Herman

The journalist downloads the encrypted submission on a Journalist Workstation, moves it on a USB drive to an air-gapped Secure Viewing Station, a laptop running Tails from a USB stick, and decrypts and reads it there. That was the classic workflow. Was, because it's going away. The migration documentation says the Tails-based setup has transitioned out completely in favour of Qubes-based Workstations, you can administer from a Qubes Admin Workstation as of late this year, and the Tails version loses support after the end of 2027.



Corn

Walk me through what the Qubes machine actually is, because I think people hear "one laptop instead of two" and think it got simpler.



Herman

It did not get simpler. It got denser. SecureDrop Workstation is a single laptop running Qubes OS, and Qubes does security by isolation. The work is split across virtual machines that are only allowed to do one thing each. sd-app runs the SecureDrop Inbox and holds the decrypted messages, and it has no network. sd-viewer is the template for disposable viewer machines, no network. sd-gpg holds the decryption key, no network. sd-proxy is the one machine that can reach the server, and only through Tor. And underneath all of it, dom0, the Qubes host, has no internet at all.



Corn

So the machine that runs the other machines can't phone anyone.



Herman

Can't reach anyone. Documents open in disposable machines that are destroyed when you close them. Copy and paste between the SecureDrop machines is disabled. Updates apply automatically before login. The machines run custom grsecurity-patched kernels, from the hardened-kernel project.



Corn

The clipboard is off. That's the detail that tells you who this is for.



Herman

It tells you what they're worried about, which is a document that wanders. The origin story, Swartz, Poulsen and DeadDrop, plus why PGP defeated Glenn Greenwald, was part one, so I'll skip it. What matters here is the current machine. Development on the Workstation started in 2017 and it only left pilot stage in 2024. That's close to a decade of engineering on the reading side of one inbox.



Corn

Now the bill. What does that rigour cost an organisation, in the boring sense?



Herman

Hardware, mainly. The Qubes machine needs a sixty-four-bit Intel processor with virtualisation support and at least thirty-two gigabytes of RAM. A lot of organisations had to buy new laptops. And the ones whose staff use YubiKeys were told not to migrate yet, because YubiKeys aren't supported on the Qubes workstations.



Corn

You're a newsroom on a deadline and the secure option requires a new laptop and breaks your two-factor keys.



Herman

For now, yes. And that friction is exactly where the institutional line sits. An organisation with a support contract and a training programme absorbs that. It's a line item and a staff memo. A self-deployed organisation reads "thirty-two gigabytes of RAM" and quietly stays on the old thing until it's unsupported.



Corn

Quietly being the operative word.



Herman

Nobody announces they're behind. They just are. And to be fair to the project, this is what supported looks like in practice. The server is on 2.16.2, released late October, with earlier releases in February, April and June. Last year the server moved from Ubuntu 20.04 to 24.04 through a fully automated migration. The Workstation dropped Whonix in favour of plain Tor, added driverless printing, and the admin tool now ships as a Debian package.



Corn

Driverless printing feels like a strange feature to brag about in this company.



Herman

It's for the poor reporter who has to print one page in a room with no network. Everything in that feature list is somebody's Tuesday.



Corn

There's a new client too, isn't there.



Herman

The SecureDrop Inbox, announced in April. A full rewrite of the legacy client, built with Electron, and X41 did a security audit of the Electron app the same month. Whether you trust Electron in a hardened environment is a whole argument, but the point is they rewrote the thing people actually touch, and an outside firm audited it.



Corn

Who's actually running it? The directory is opt-in, which I assume means it's a floor, not a census.



Herman

It's a floor. The public directory on securedrop dot org lists twenty-four entries, a couple of them individual journalists. The New York Times, The Washington Post, The Guardian, ProPublica, the Financial Times, Der Spiegel, Süddeutsche Zeitung, The Economist, CBC, The Globe and Mail, Bloomberg News, Forbes, the Norwegian and Swedish outlets, Forbidden Stories, Whistleblower Aid, Greekleaks. But opt-in means many run unlisted, and an older Tor Project page said more than sixty major news organisations. No authoritative total count exists, and I wouldn't trust anyone who claims one.



Corn

Twenty-four names on the door, some unknown number behind it. That's an honest answer, and it's rarer than it should be.



Herman

Daniel asked for an audit, so audit honesty applies.



Corn

One thing before we leave SecureDrop. The servers sit on the newsroom's own premises. Compare that with the commercial platforms, which are mostly vendor-hosted SaaS, and the Qubes rig is designed to keep even the newsroom's own network out of the loop.



Herman

Premises, air gaps, and the assumption that anything networked is eventually an enemy. SecureDrop is the newsroom model. GlobaLeaks is the other open-source institution-grade model, and its shape is different in a way that tells you who it's for.



Corn

Go on.



Herman

It's developed by the Hermes Center for Transparency and Digital Human Rights in Italy. The project started in December 2010, first prototype announced September 2011, and the current release came out at the end of October. It does Tor onion services, like SecureDrop, but it also does ordinary HTTPS, and that's the key institutional difference. A public body needs a reporting channel that ordinary citizens can reach, people who will never install Tor Browser. That's a completely different threat model from a newsroom's source, and GlobaLeaks serves it.



Corn

The newsroom optimises for the source who is terrified. The public authority optimises for the citizen who is ordinary.



Herman

And GlobaLeaks adds configurable questionnaires and data retention limits, which matter when you're a government body with legal obligations about what you keep and for how long.



Corn

Who uses it? I remember it from the collective leak-site era.



Herman

Publeaks in the Netherlands, 2013, built with Free Press Unlimited and about twenty Dutch media organisations. Then MexicoLeaks, IndonesiaLeaks, Filtrala in Spain, PeruLeaks. Those were the media collectives. But the bigger story is public authorities. ANAC, the Italian National Anticorruption Authority, launched its national whistleblowing platform on GlobaLeaks with onion services in 2018. A national anticorruption authority running open-source software with a Tor option, that's about as institution-grade as open source gets.



Corn

And the counts of Italian public bodies on it, those are the numbers I'd want a caveat on.



Herman

Every single one of them. WhistleblowingPA is the free platform for Italian public bodies that Transparency International Italia launched with GlobaLeaks in 2018. How many bodies use it? Roughly two thousand on one undated Transparency International profile. More than five thousand on GlobaLeaks' network profile. Seven thousand public agencies in an interview with GlobaLeaks' Giovanni Pellerano last year. And GlobaLeaks' own site says more than ten thousand public entities in Italy, but that's self-reported and wider than WhistleblowingPA alone.



Corn

Somewhere between two thousand and ten thousand, depending on who you ask and when.



Herman

And that spread is itself the finding. Nobody disputes that it's a lot. Nobody can tell you how many, because there's no registry, just vendors and NGOs counting their own footprints.



Corn

For a tool whose entire job is verifiable reporting, the deployment numbers are the least verifiable thing about it.



Herman

Beyond Italy, the named adopters include Barcelona City Hall, the Valencian Antifraud Authority, the German Federal Office of Justice, the Greek National Transparency Authority, the Danish Data Protection Authority, and BIANCO, Madagascar's anti-corruption agency.



Corn

Now the Directive, because that's the hinge for the commercial side. Twenty nineteen?



Herman

Directive 2019/1937 entered into force on the sixteenth of December, 2019. Transposition deadline was December 2021, with extra time to December 2023 for internal channels at private companies with fifty to two hundred forty-nine workers. Article 8 requires private entities with fifty or more workers, and public bodies, to run internal reporting channels. Member states can exempt small municipalities. Firms in the fifty to two hundred forty-nine band can share a channel, which was a concession to cost. Financial-sector entities are covered regardless of size.



Corn

And the deadlines that give the whole commercial market its shape.



Herman

Acknowledgement within seven days. Feedback within three months. Those two numbers are why the platforms look the way they do. Whether anonymous reports must be accepted is left to member states, so it differs by country. And by April of this year, all twenty-seven member states had finally passed transposing laws, roughly four years late, and per the EU Whistleblowing Monitor, none of them could yet be called fully compliant. The Commission's own report in 2024 found widespread conformity problems, and infringement cases went to the Court of Justice.



Corn

Everyone passed a law. Nobody got it fully right.



Herman

Which means the tooling is arguably ahead of the institutions using it. That's the whole commercial market, though, because a company that suddenly must acknowledge in seven days and feedback in three months, and has never run a channel in its life, goes shopping.



Corn

Let's hear from a listener before we get to what they find. This is Beryl from Leeds. Beryl: Hello, it's Beryl from Leeds, I'm sat in the car outside the supermarket with the engine off because I didn't want the beeping to get on the tape, and I've been thinking about your whistleblowing episode all week. I think the thing I keep coming back to is, you said the real line is between supplied and supported and self-deployed, and that makes a lot of sense to me, but I wondered whether you'd say owt about what happens to the person after they've sent the thing in. Because my nephew works in compliance at a council and he says the hardest part isn't the software, it's that nobody tells the whistleblower anything for months and they start to feel like they've been quietly ignored. Anyway, that's my question, thanks, love the show.



Herman

Her nephew is describing the exact gap the Directive's deadlines were meant to close, and the exact thing the commercial platforms actually sell. Seven days, three months. Whether anyone meets them is a different question, but at least there's a clock with a name on it now.



Corn

A channel that exists on paper, and a person somewhere who dreads opening it.



Herman

And that person's employer buys software. Back to the audit. EQS Integrity Line, formerly Got Ethics, from EQS Group in Munich. Thoma Bravo took EQS private, offer announced November 2023 at forty euros a share, settled February 2024, shares delisted May 2024. Their own pages claim twenty-five hundred customers for Integrity Line, or four thousand, depending on the page, and fourteen thousand for the whole group.



Corn

Their own marketing disagrees with itself by about sixty percent.



Herman

NAVEX is the other giant. EthicsPoint handles hotline and web intake, they target large enterprises, and they don't publish prices at all. They bought the Stockholm-based provider WhistleB in December 2019, and in October 2025 a consortium led by Goldman Sachs Alternatives, including Blackstone, completed a majority stake acquisition. That's a private equity firm and a bank buying the intake layer for corporate misconduct reports.



Corn

Whispli is the smaller one, isn't it.



Herman

Founded around 2015, generally listed as Sydney-based, more than three hundred customers in over sixty countries, all self-reported, a SOC 2 Type 2 certification claimed, positioned at the mid-market. And Vault Platform, London-based startup, raised about twelve point four million dollars, was acquired by Diligent in May 2025 and folded into Diligent's governance, risk and compliance suite. So it's no longer an independent vendor at all.



Corn

The pattern in those two deals is the interesting part. Vault absorbed into a GRC suite, NAVEX under Goldman Sachs. The category is consolidating into general corporate compliance machinery.



Herman

And I want to defend the commercial side here, because Daniel's framing is right. It's tempting to see EQS and NAVEX as the boring corporate versions of the real thing. But look at what they actually sell. Triage. Investigator workflow. Audit trail. Hotline. Multilingual intake. Compliance reporting. That is exactly what an organisation needs to meet a seven-day acknowledgement and a three-month feedback deadline. The anonymous inbox is almost the least interesting part of what they sell.



Corn

Say more about the triage part, because I don't think people picture what that actually is.



Herman

Picture a multinational with reports coming in in six languages, some anonymous, some not, some about expense fraud, some about safety. Somebody has to route each one to the right team, record every action taken, prove later who saw what and when, and close the loop with the reporter inside the deadline. That's not cryptography, that's case management, and doing it badly is how reports about safety end up filed under expenses for four months. The commercial platforms are, in large part, deadline machinery.



Corn

SecureDrop sells paranoia, in the best sense. EQS sells paperwork, also in the best sense.



Herman

Both are operational competence, bought rather than built. Which takes us to Daniel's last question, what happens to a leak once it arrives.



Corn

Three different answers.



Herman

Three. On SecureDrop, the source gets a randomly generated codename, which is the only credential they have, and the leak lands encrypted on a server the newsroom controls. The journalist can reply through the same system, so the source never needs to hand over an email address. The verification work is journalistic: corroborating the documents, checking their metadata, asking the source questions through that same channel. And documents from an unknown sender get opened only in the disposable viewer machines, never in a normal environment. The operational security is the isolation we walked through. On GlobaLeaks, the leak lands in a configurable questionnaire with retention limits, and the operational security is whatever the deploying body configured, which is exactly where supported deployments diverge from self-hosted ones. On the commercial platforms, the leak lands in a case management system with an audit trail, and the verification is an investigator's workflow with deadlines attached.



Corn

The common thread is that receiving the leak was never the hard part.



Herman

In every family, the hard part is what the institution does next. And that's precisely the part the supplied-and-supported players are selling, whether the supplier is the Freedom of the Press Foundation or a compliance vendor in Munich.



Corn

Before we wrap the audit, the forward-looking wrinkle.



Herman

The SecureDrop Protocol. A paper this year from Freedom of the Press Foundation researchers and ETH Zurich. It proposes end-to-end encryption, hybrid post-quantum security, identity-hiding message fetching, and deniability, all aimed at allowing cloud-based deployment. The Foundation plans to deploy it, with integration starting this year. It's not the live system, I want to be clear about that.



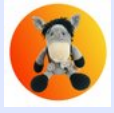
Corn

The most air-gapped tool in the world is drafting its own move to the cloud. That would change this whole calculus again.



Hilbert

Herman, how much RAM did you say that Qubes laptop wants?



Herman

Thirty-two gigabytes.



Hilbert

I had one. Sold it last spring. I'd gone through a stretch of setting up viewing stations for people who'd bought the support contract and then found nobody on staff could follow the instructions, and the one machine I kept was the demo laptop. The staff at the last place kept getting the USB order wrong, moving the drive to the air-gapped box before the transfer had finished, so I had a card laminated with the order of operations and taped it to the wall of that room. Ten steps. Numbered. Corn will like this, it was the only document in the building nobody was allowed to take out.



Corn

Of course it was.



Hilbert

I still have a copy of the card. It's in a drawer. I never threw it out, and after your supplied-and-supported business today I think it's the most honest thing ever written about whistleblowing. The contract was paid, the training was included, and the wall held the only instructions anyone actually followed. I did a stint years back maintaining evidence recorders, same problem there. The machine was never the weak part.



Herman

That supported-but-ignored category, the paid contract with nobody trained, is real, and it's the one gap in the frame we built. You can buy the support and still only use the helpdesk.



Corn

The card lasted longer than the training. That's the audit finding nobody publishes.



Hilbert

The card outlasted the department, actually. There was a reorganisation.



Herman

There's always a reorganisation.



Corn

The misconception I'd want to kill before we close, because I hear it constantly, is that SecureDrop is still the Tails USB stick and the air gap. It isn't. The project has moved completely to Qubes-based Workstations, and the Tails version stops being supported after the end of 2027.



Herman

Right, and the related one, that the commercial platforms are the real stuff and open source is the hobbyist option. A neglected self-deployed open-source instance is worse operationally than a supported commercial one, and a vendor-hosted SaaS box is not automatically less trustworthy than a server nobody patches.



Corn

So where does this leave the open question?



Herman

The one I can't shake is all those channels that were stood up to satisfy a deadline and then left alone. Transposition is complete on paper, twenty-seven out of twenty-seven, and the monitors say none is fully compliant. Behind that sit countless internal channels stood up to meet a deadline, some well supported and some on the strength of a laminated card.



Corn

And the SecureDrop Protocol's move toward cloud would blur the air-gap story that defined the newsroom side for a decade, while the commercial market consolidates into private equity hands. The supplied-and-supported category gets narrower, more corporate, and more capable all at once.



Herman

Which is the whole reframe, really. The interesting question was never the licence. It's who is standing behind the tool when the leak arrives, and whether the institution has the competence to do anything with it once it does.



Corn

Next in the series we leave the supplied-and-supported world and look at the tip lines smaller organisations run themselves.



Herman

Where the question of who is standing behind the tool gets a lot more personal.