Episode Book

EPISODE #6572

When Encryption Friction Nearly Stopped the Snowden Leak

PUBLISHED	13 November 2026 at 21:52 UTC
DURATION	27:42
LISTEN	myweirdprompts.com/episode/whistleblowing-encryption-usability-friction-73435/
HOSTS	Corn, Herman, Desmond, Hilbert
SCRIPT MODEL	z-ai/glm-5.3
VOICES	chatterbox-regular (chatterbox-local)
PIPELINE	V5.26
SOURCES	15 cited by the research (listed at the end)
BOOK GENERATED	14 November 2026 at 06:47 UTC

SYNOPSIS

Edward Snowden's first anonymous approach to Glenn Greenwald stalled for months because Greenwald wouldn't install PGP, even after watching a 12-minute video tutorial. That friction exposes a deeper flaw in whistleblower tools: a 1999 study found only two of twelve experienced email users could correctly encrypt a message, and the 2020 paper 'Snitches Get Stitches' argues most leakers face small workplace anonymity sets rather than the NSA. Also covered: Laura Poitras's operational response and SecureDrop's origins.

TRANSCRIPT



Corn

The biggest leak of the century nearly died because one journalist couldn't install software. That's where Daniel wants us to start.



Herman

It really is the perfect opening for this. He sent us a long note about whistleblowing technology — he's kicking off a whole series on it, and he begins with the story that stuck with him: Edward Snowden's first anonymous approach to Glenn Greenwald, the PGP setup that never happened, and the question underneath it — we build elaborate secure systems for leaking, but most whistleblowers and plenty of journalists aren't technical. How much does that friction cost, how many sources quietly give up or fall back to a personal email or a phone call, and what has the field actually learned about designing security a frightened, ordinary person will use?



Corn

He also wants the series framed — this is part one, the usability-versus-security tension, and later episodes get into the tools, the tip lines, AI as an anonymiser. For today, we start with the failure that almost stopped the story before it began.



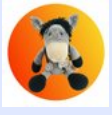
Herman

So let's set it up properly. Early twenty thirteen — the reporting says January or February — an anonymous email arrives for Glenn Greenwald. It's signed Cincinnatus. The sender says he has information of great interest and asks to communicate using PGP encryption.



Corn

And Greenwald wrote back that he did not have such software.



Herman

That's the NYT's wording, yes. "Mr. Greenwald wrote back that he did not have such software." And Snowden — patient, remember, this is a man who had planned this for a long time — sends him a step-by-step written guide. Then, when that doesn't land, a homemade video tutorial. Twelve minutes long, diagrams, an obfuscated voice, walking Greenwald through installing PGP step by step.



Corn

Twelve minutes. I've spent longer than that deciding which leaf to eat.



Herman

Greenwald watched it. The Washington Post's headline when the video surfaced publicly in twenty fourteen was blunt — "Edward Snowden sent Glenn Greenwald this video guide about encryption for journalists. Greenwald ignored it." Watched, never completed the setup.



Corn

That's the detail I want to sit on, actually. Not that he couldn't — that he watched a personal tutorial made by an NSA insider and still didn't finish the install. What was the calculus there?



Herman

I think it's exactly what it looks like. Greenwald is a lawyer, a Pulitzer-winning journalist — this is not a man who can't follow twelve minutes of instructions. But think about his position in January twenty thirteen. He gets anonymous emails fairly often. Ninety-nine out of a hundred are cranks. The video is interesting, sure, but setting up PGP is an evening of friction for a claim with an unknown probability of being real. The expected value calculation says wait.



Corn

"I'll do it if he turns out to be real" — which you can only find out by not doing it.



Herman

There's a paper from twenty twenty, "Snitches Get Stitches" — Ahmed-Rengers, Anderson and others — that formalizes exactly this. Their line is that the whistleblower is often "at the mercy of motivations and abilities of others." Snowden could be the most careful, most technically brilliant source in history, and the whole thing still turns on whether one particular recipient feels like doing homework.



Corn

So the source's security is outsourced to the laziest link in the chain.



Herman

The interesting turn is who picked it up. Laura Poitras — the documentary filmmaker — got an anonymous request for her public encryption key in January of that same year. She'd been filming a surveillance documentary for nearly two years, she got queries like this occasionally, she sent her key and, by her own account, didn't think much would come of it.



Corn

Then the stranger escalated.



Herman

He sent instructions for an even more secure system, and told her to pick long passphrases, and gave her the threat model to assume: "Assume that your adversary is capable of a trillion guesses per second." She decrypted the message, and — this is Peter Maass's account in the New York Times Magazine — seconds after reading it, she disconnected from the internet and removed the message from her computer.



Corn

She didn't just read the email well. She responded operationally, within seconds.



Herman

And she still thought it might be a trap. She confronted the sender directly: either you have this information and you're taking huge risks, or you're trying to entrap me and the people I know, or you're crazy. Greenwald, meanwhile, called her the Keyser Soze of the story — completely invisible and yet ubiquitous.



Corn

What I find telling is what she said about her own limits. She already had keys, right?



Herman

She did. She'd filmed with WikiLeaks, she knew Jacob Appelbaum, and here's the part that matters — after her filming in Iraq she'd been detained and searched at airports repeatedly, and she'd responded by routinely wiping her computers and phones. Her security literacy wasn't academic, it was earned at a border. And even she said what Snowden was asking for was "beyond what I was using in terms of security and anonymity."



Corn

So the bar was: the one journalist in America with hard-earned operational security habits found the requested setup demanding. The system's floor was above nearly everyone's ceiling.



Herman

Which raises the obvious question — was this a one-off, or is the tooling just like this? And the answer is documented, and it's worse than you'd guess. Nineteen ninety-nine, USENIX Security Symposium, Alma Whitten and J.D. Tygar, a paper called "Why Johnny Can't Encrypt." They took PGP five point zero, twelve experienced email users, ninety minutes each, one task: sign and encrypt a message in a simulated campaign scenario.



Corn

Twelve people, ninety minutes. That's generous.



Herman

Extremely. Results: three of the twelve accidentally emailed the secret unencrypted. One couldn't encrypt at all. Seven — this is my favorite number in the whole paper — seven encrypted successfully but only with their own public keys, which means they locked the message so that only they themselves could read it. Two, out of twelve, eventually sent correctly encrypted email.



Corn

Seven people performed a security ritual perfectly and secured the message against the intended recipient.



Herman

And here's the kicker — the twenty twenty paper looked at the New York Times's own recommended workflow for sources, the Mailvelope browser-plugin PGP setup, and noted it "exhibits similar properties to those that confused most users in the canonical paper of security usability." The advice sources were being given in the twenty-tens reproduced a documented nineteen-nineties failure, almost exactly.



Corn

The field knew for fourteen years and shipped the homework anyway.



Herman

Greenwald did eventually get there — the reporting says by late April or early May of twenty thirteen he and Snowden were on an encrypted chat program. So the friction delayed the channel, it didn't kill it. But "the biggest leak of the century arrived two months late because of an installer" is not a comforting margin.



Corn

Let's take Daniel's harder question, then — the cost of that friction in aggregate. How many sources give up?



Herman

Nobody knows. And I want to be precise about that, because it's not a shrug — it's a finding. There is no published figure anywhere for how many would-be sources abandon a secure channel, or bounce at the Tor download, or fall back to their personal email or a phone call. You can find lab failure rates, you can find SecureDrop's own open research questions about whether sources understand their codename screen — do they memorize it, write it down, ignore it — but those questions have been sitting on their UX wiki since twenty eighteen without published answers. The attrition funnel is invisible.



Corn

That's the piece that should embarrass somebody. The field can measure whether twelve grad students can encrypt, but the actual leak pipeline — the thing the tools exist for — has no numbers.



Herman

And it's measurable in principle, or at least approximable. Newsrooms know how many submissions arrive through insecure channels. The problem is nobody wants to publish their insecure-channel volume, because it's an admission.



Corn

Every unpublished number in security is an admission of something.



Herman

Here's where the twenty twenty paper does something I didn't expect, though. Instead of trying to estimate the attrition rate, it attacks the premise. Their argument: the Snowden case represents a tiny minority of whistleblowing situations. Usually the adversary is not the NSA. It's a medium-sized business, or a public-sector body like a hospital. The whistleblower is not an expert in anonymity. And — this is the crucial part — the anonymity set is not tens of thousands of NSA technical staff. It's the handful of people who knew what was going on. Sometimes it was just one person.



Corn

Say that plainly for anyone who hasn't thought about it. The anonymity set is the group of people who could plausibly have leaked.



Herman

Right. If three people in a hospital knew what was in that document, and a leak appears in the paper, the hospital doesn't need to break Tor or defeat PGP. It needs to look at the other two people. The tool choice is almost beside the point — the elaborate crypto stack protects against an adversary most whistleblowers don't face, while the actual risk, being suspected by the people you work with, walks straight past it.



Corn

Which flips Daniel's question. He asked how much the friction costs. If the anonymity set is three people, the friction costs everything and the encryption buys almost nothing.



Herman

The paper reviewed case studies from a UK whistleblowing charity, Public Concern At Work, and found the small-anonymity-set situation was the norm, not the exception. There's a UK construction-industry blacklist in that literature — over three thousand people, union activists and whistleblowers, shared quietly among employers for years. No cryptographic adversary anywhere in that story. Just people with files.



Corn

Before we go further — we're getting into the cost of friction, and Desmond has his regular segment.

D

Desmond

Desmond's Money Tip. When a birthday card comes through the post, sign it back, cross out their name, and send it again next year. That is one card, one stamp, and one envelope saved per person per year, which is about four pounds fifty annually, or two hundred and twenty five pounds over a lifetime, assuming you live another fifty birthdays, which is optimistic.

D

Desmond

I keep a drawer of used cards sorted by sender, and I have not bought a card since two thousand and eleven. It is not much, but it is money you still have.



Corn

I'm honestly considering the drawer.



Herman

Please don't. You know what — the blacklist is actually the thing I can't shake. Three thousand people, and the mechanism that caught them wasn't metadata, it was a spreadsheet someone maintained in an office. Anyway — if the adversary is usually a hospital administrator and not the NSA, what does that mean for everything the field built? Because the field did build something. Have you looked at SecureDrop's history?



Corn

I know the outline. Aaron Swartz and Kevin Poulsen, DeadDrop — and I know the name changed after Swartz died in January twenty thirteen.



Herman

That's right — James Dolan is also credited as a co-creator. Swartz died on January eleventh, and the first public instance of the code launched that May as Strongbox at The New Yorker. The Freedom of the Press Foundation took over development, renamed it SecureDrop, formal release October twenty thirteen. It's still actively maintained — current stable release came out just a couple of weeks ago.



Corn

Walk me through the design, because the design is the argument.



Herman

It's a Tor-only onion service. On the source side, the whole burden is: open Tor Browser, visit the onion address, and you get a randomly generated codename. Remember the codename, come back with it, that's your identity. No account, no email, nothing traceable to you by design. The project even advises sources to disable JavaScript.



Corn

And on the journalist side?



Herman

Here's where it gets heavy. Two USB drives, two computers. The second machine is air-gapped — never touches the network — and wiped on every reboot, with the decryption code living on the second drive. The submission moves from the networked machine to the air-gapped one physically, by USB, and the secure machine forgets everything each time it restarts.



Corn

So the design decision, stated out loud, is: the source gets a codename and the newsroom gets a small priesthood.



Herman

That's the fairest one-line version I've heard. And it's deliberate — the philosophy is that the frightened non-technical person is the one who can't be asked to absorb complexity, because they'll bounce. Push the difficulty to the side that's paid, staffed, and can be trained. But the journalist-side burden is heavy. The project's own UX designer, Nina Alter, described the multi-device workflow as "an ongoing, known pain point for journalists using SecureDrop" — and one that imposes real cost barriers on smaller newsrooms that can't spare two dedicated machines and a person to manage them.



Corn

Herman, you've installed things in this flat your whole life. Two air-gapped machines, wiped on reboot — how long before the third journalist on the roster just checks her Gmail?



Herman

That's exactly the right question, and there's a measured answer, which is rare in this space. The SecureDrop Workstation project — a dedicated, hardened workstation product built on Qubes — brought active journalist time on task down from roughly forty-five to sixty minutes of hands-on work to roughly five to fifteen minutes.



Corn

From an hour to a coffee break.



Herman

Across three organizations and eight journalist users, so small numbers, be careful with it — but a three to four times reduction is real. The part I keep coming back to is what it took. That improvement arrived roughly a decade after launch, and it required a dedicated workstation product with its own hardware assumptions. The fix for "this is too much work" was a decade of engineering.



Corn

Better is real, but the ledger reads: source friction down, newsroom friction down by three-quarters, time to deliver the reduction, ten years.



Herman

Adoption tells you the newsrooms thought it was worth it. More than sixty-five news organizations globally. The New Yorker first in twenty thirteen, then Forbes, ProPublica, The Intercept, the Washington Post and The Guardian in June twenty fourteen, then the AP and the Times in late twenty sixteen, BuzzFeed News, USA Today, ABC Australia... And the Freedom of the Press Foundation committed to independent third-party audits before every major release — the first by University of Washington researchers with Bruce Schneier, the second by Cure53.



Corn

Sixty-five organizations is the upside. What fraction of the world's newsrooms is that, would you guess?



Herman

Tiny. Most regional and local outlets, most non-English newsrooms, nothing. Which matters because the small-anonymity-set whistleblowers — the hospital, the mid-sized firm — are exactly the ones whose local paper has one IT person who also fixes the printer.



Corn

The audit trail has a nice irony, though. The tool exists because a journalist wouldn't follow a tutorial. Its adoption required newsrooms to follow much worse tutorials.



Herman

They did, though — that's the thing. Credit where due. And the field's honesty about its own open questions is better than most. The UX wiki from twenty eighteen lists them in almost embarassing plainness: do sources understand the codename screen? "What do they do with the codename: memorize, write it down, ignore it?" Do they grasp what Tor is doing for them, or the messaging about deleting messages to protect their privacy?



Corn

Those are research questions. Have they been answered?



Herman

Not publicly. FPF closed a call in twenty twenty-three for remote user-research interviews with past and present SecureDrop users — forty-five to sixty minutes, conducted over Signal — about how newsroom security practices changed after COVID. The findings haven't been published. So the pattern holds: the questions are asked in public and answered nowhere.



Corn

Meanwhile, what does a source actually encounter when they don't find a SecureDrop? They find the newspaper's tip page.



Herman

And this is where the twenty twenty paper is brutal. They audited newspaper tip pages, including the New York Times's, and found the guidance "lacking — indeed hazardous." The Times page lists WhatsApp, Signal, physical post, email. It does not explain what metadata is, or how it can allow the FBI to track the leaker. It never tells users that WhatsApp's anonymity set is much larger than Signal's because of sheer user numbers — which is the single fact a source most needs, because it determines whether using the app at all flags you.



Corn

The page recommends tools without telling you the one thing that decides whether the tool helps.



Herman

The paper's proposed rewrite is the model of what plain language should do: "If you're one of only six people with access to this document it might not be wise to use Signal if none of the other five ever do." One sentence. It contains the whole anonymity-set argument.



Corn

That sentence should be on every tip page in the world. It won't be.



Herman

They flag subtler traps too. Smartphone apps may link the leak to a specific phone number — and changing your SIM card may not help if the change itself is flagged as suspicious. There's a side-channel I find creepy: DNS is widely monitored for malware detection, so a machine that resolves the address of a commonly-used leak-tool plugin can be flagged as suspicious — especially just after that machine accessed the New York Times.



Corn

So the sequence "visited the paper's tip page, then looked up a privacy tool" is itself the evidence. You don't need to read the message to know a message was probably sent.



Herman

On physical post, the Times page recommends a public mailbox rather than a post office, but never says why — and the why is that the US government scans all snail mail and records sender and destination. And printers: identifying watermarks, and on-device storage that's hard to clear. The page sends you down routes it doesn't explain, with hazards it doesn't name.



Corn

We did an episode on this, actually — the messaging-app privacy one, where we went through what your app leaks before anyone reads a word. Metadata was the whole spine of it, and here's the Times doing exactly the thing we complained about: a security recommendation with the security left out.



Herman

The deeper argument the paper builds to is the one I'd take issue with you about, though — or want your view on. The authors say they set out "to find a better technological solution, but soon realised we were missing the forest for the trees. Technology plays a small part in a much larger game." Their word for the disease is technical solutionism. And their counter-example is Harvey Weinstein and #MeToo. Eight women paid off over some thirty years, and the dam didn't break because someone built better encryption. In their words, the key was "a shift in soft power that gave victims and witnesses the confidence to tell their stories."



Corn

Meaning the binding constraint wasn't secrecy, it was believing you'd be believed.



Herman

That's it. Once the first stories were believed, the second and third came without any new tool at all. The tool that mattered was momentum.



Corn

I half buy it. Let me push the other half. #MeToo sources weren't leaking documents — they were testifying to experience. There's no codename problem when your evidence is your own memory. A hospital whistleblower with a memo has a different physics: the memo itself points back at the three people who had it.



Herman

That's fair — and the paper acknowledges the difference by implication, honestly. They also cite the case of a breast surgeon who subjected over a thousand patients to unnecessary operations across fourteen years before being stopped. Internal channels failed there for fourteen years, and it wasn't because anyone lacked Signal. So I'd put it this way: the soft-power constraint decides whether anything happens; the tooling decides who pays for it happening.



Corn

Hmm. That's better than my objection. The tools don't unlock the leak, they price the whistleblower's risk.



Herman

And then the Greenwald story slots in neatly — the one case where the adversary really was the NSA, the anonymity set really was huge, the cryptography really was load-bearing. And even there, the lot hinged on whether one lawyer would finish an installer. That's the "mercy of motivations and abilities of others" line again. Even the best case is somebody else's homework.



Hilbert

The Greenwald delay was two months, not the winter. He was encrypting with Snowden by late April.



Herman

Late April or early May — that's the reporting, yes.



Hilbert

I had a run at this myself, Corn. Few years back I had something I wanted a journalist to have. Not state secrets — a supplier's ledger I'd ended up holding, long story, the man had been shorting the till on returns for years and I'd kept the paperwork because I don't throw away paperwork. I sent the newsroom their secure portal link request like a civilized person and what came back was a reply from the journalist's personal Gmail saying just email it over. Three days I sat on that. Couldn't work out whether it was laziness or a trap, because those look identical in an inbox. I know what you're going to say about the metadata, Herman — you spent a whole segment on it earlier and you were right, that's the bit that gets people. Gmail was out. So I copied the ledger onto a USB stick, put it in a padded envelope with a note that said "for the journalist," and posted it. Ordinary postbox, near my house.



Corn

Not a public mailbox across town.



Hilbert

Near my house. I stand by that part less now. The Gmail reply is still on my laptop, in a folder called evidence. I check it now and then to see if the account is still active. It went quiet about a year ago, which I have noted and am watching. Anyway. The story ran, small piece, page eleven, and the supplier paid back what he owed over eighteen months.



Hilbert (continued)

Nobody went to prison. The journalists did their work properly once they had the thing in their hands, I'll say that for them.



Herman

The interesting part of your story is that your decision not to use the insecure channel took three days of a careful man's attention, and the secure alternative took one envelope and no tools at all. The USB stick was the low-friction option.



Hilbert

It was the option I could finish before lunch, Herman. That's most of what a secure channel turns out to be, if you want my... no, I'll leave it there. The work got done.



Corn

He's not wrong, and I resent it.



Herman

The ledger got there and the man paid back the money — that's a better outcome than most of the case studies we've cited today. Anyway — where we've landed is uncomfortable, and I think it's the honest place for an opening episode. The field documented PGP's unusability in nineteen ninety-nine, shipped it as the recommended workflow into the twenty-tens anyway, then spent a decade engineering SecureDrop down to a coffee break of journalist time — and the twenty twenty paper's conclusion hovers over all of it: the main constraints are often institutional.



Corn

And the question the series keeps running into is whether the friction was ever the real wall. Hilbert's envelope did more work than his three days of deliberation.



Herman

Cutting-room floor, before we go — the detail from today's reading that didn't fit anywhere. Poitras's response to the airport detentions: she'd been routinely wiping her computers and phones after every crossing, for years, as a habit. Not a security product, not a tool — a ritual. When the literacy finally mattered, it was already muscle memory. And the blacklist number I keep thinking about: three thousand people on that construction-industry list, held quietly among employers, and not one line of cryptography was involved in catching any of them.



Corn

A spreadsheet outperformed the entire crypto stack, and a woman with a wipe habit outperformed a Pulitzer winner with a tutorial.



Herman

So the open question I'd leave for the series: if the anonymity set is usually three people and the binding constraint is soft power, what is the next decade of whistleblowing technology actually for? SecureDrop pushed the difficulty to the newsroom and spent ten years shrinking it — was that the right relocation, or did it just move the pile? And after all these years, why does nobody publish the attrition number? The one figure that would tell us what the friction costs has never been counted, and I don't think that's an accident.



Corn

If you want to hear where the series goes — the tools, the tip lines, AI as an anonymiser — subscribe and leave a review, it helps people find the show. Our producer is Hilbert Flumingtop, who as established does not throw away paperwork. For more along these lines, there's episode ten, How ASR Went From Frustration To ... Whisper Magic; and episode eight, Building Your Own Whisper. This has been My Weird Prompts — no question too obscure, no rabbit hole too deep. Find everything 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. **Ahmed-Rengers, Anderson, Halatova et al., Snitches Get Stitches: On The Difficulty of Whistleblowing, LNCS 2020 (arXiv:2006.14407); retrieved 2026-11-13. [primary]**

   https://arxiv.org/abs/2006.14407

2. **Whitten & Tygar, Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0, 8th USENIX Security Symposium, August 1999; retrieved 2026-11-13. [primary]**

   https://www.usenix.org/conference/8th-usenix-security-symposium/why-johnny-cant-encrypt-usability-evaluation-pgp-50

3. **full text of the Whitten/Tygar paper, test design and results; retrieved 2026-11-13. [primary]**
https://www.usenix.org/legacy/events/sec99/full_papers/whitten/whitten_html/

4. **FPF SecureDrop UX wiki, 2018-09-24; retrieved 2026-11-13. [primary]**
https://github.com/freedomofpress/securedrop-ux/wiki/Things-We-Want-To-Learn-About

5. **Freedom of the Press Foundation, user research call, closed 2023-07-27; retrieved 2026-11-13. [primary]**
https://securedrop.org/news/securedrop-is-evolving-we-want-to-hear-from-you/

6. **Peter Maass, How Laura Poitras Helped Snowden Spill His Secrets, New York Times Magazine, 2013-08-18; retrieved 2026-11-13.**
https://www.nytimes.com/2013/08/18/magazine/laura-poitras-snowden.html

7. **Dan Goodin, Ars Technica, 2013-06-11; retrieved 2026-11-13.**
https://arstechnica.com/information-technology/2013/06/guardian-reporter-delayed-e-mailing-nsa-source-because-crypto-is-a-pain/

8. **Wikipedia, last edited 2026-07-05; retrieved 2026-11-13.**
https://en.wikipedia.org/wiki/SecureDrop

9. **Andrea Peterson, Washington Post, 2014-05-14; retrieved 2026-11-13.**
https://www.washingtonpost.com/news/the-switch/wp/2014/05/14/edward-snowden-sent-glenn-greenwald-this-video-guide-about-encryption-for-journalists-greenwald-ignored-it/

10. **Daily Dot, 2014-05-13; retrieved 2026-11-13.**
https://dailydot.com/edward-snowden-gpg-for-journalists-video-nsa-glenn-greenwald

11. **Roy Greenslade, The Guardian, 2013-08-19; retrieved 2026-11-13.**
https://www.theguardian.com/world/2013/aug/19/edward-snowden-nsa-secrets-glenn-greenwald-laura-poitras

12. **WNYC On the Media, 2013-08-16; retrieved 2026-11-13.**
https://www.wnycstudios.org/podcasts/otm/segments/312932-role-model-security-savvy-journos

13. **Nina Alter, Source/OpenNews; retrieved 2026-11-13.**
https://source.opennews.org/articles/making-securedrop-easier-use-more-journalists/

14. **Nina Eleanor Alter, SecureDrop Workstation project outcomes; retrieved 2026-11-13.**
https://bigwheel.net/project/securedrop-workstation/

15. **Wikipedia, last edited 2026-11-02; retrieved 2026-11-13.**
https://en.wikipedia.org/wiki/Freedom_of_the_Press_Foundation