You received a leak, now what?

A hands-on OPSEC simulation

Alex Pyrgiotis
Freedom of the Press Foundation

Kolja Weber
FlokiNet

Aspects of a tip

1. First contact

How sources learn where to send tips.

2. GrapheneOS + Signal = ❤️

Hardening the mobile tipline

3. Perimeter security

Walls have ears, we have gears.

4. QubesOS + SecureDrop = ❤️

Compartmentalization as a defense.

5. Post-verification

Store it, share it, publish it, without burning your source.

PART I

The first-contact problem

How sources learn where to send tips.

The tipline situation in 2013

In 2013, an anonymous user contacted Micah Lee, then staff technologist at EFF and CTO at Freedom of the Press Foundation:

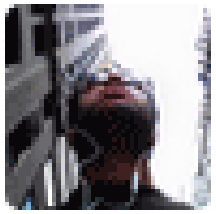
> *From: anon108@■■■■■■■■*
> *To: Micah Lee*
> *Date: Fri, 11 Jan 2013*
>
> *Micah,*
>
> *I'm a friend. I need to get information securely to **Laura Poitras** and her alone, but I can't find an email/**gpg** key for her.*
>
> *Can you help?*

Source: The Intercept — Ed Snowden Taught Me To Smuggle Secrets Past Incredible Danger. Now I Teach You.

The tipline situation in 2013

That person was paranoid enough about security that even though they acquired Laura's PGP key, they proposed Micah to tweet it, just to be sure.

> *From: 303@riseup.net*
> *To: Micah Lee*
> *Date: Mon, 28 Jan 2013*
>
> *Hey Micah,*
> *This is **Laura Poitras**.*
> *Someone is trying to verify my fingerprint to this email. The person has proposed you **tweet the fingerprint**.*
> *Would you be able to tweet this to your acct:*
> ***1EBF 5F15 850C 540B 3142 F158 4BDD 496D 4C6C 5F25***
> *Let me know if possible.*
> *Thanks,*
> *Laura*



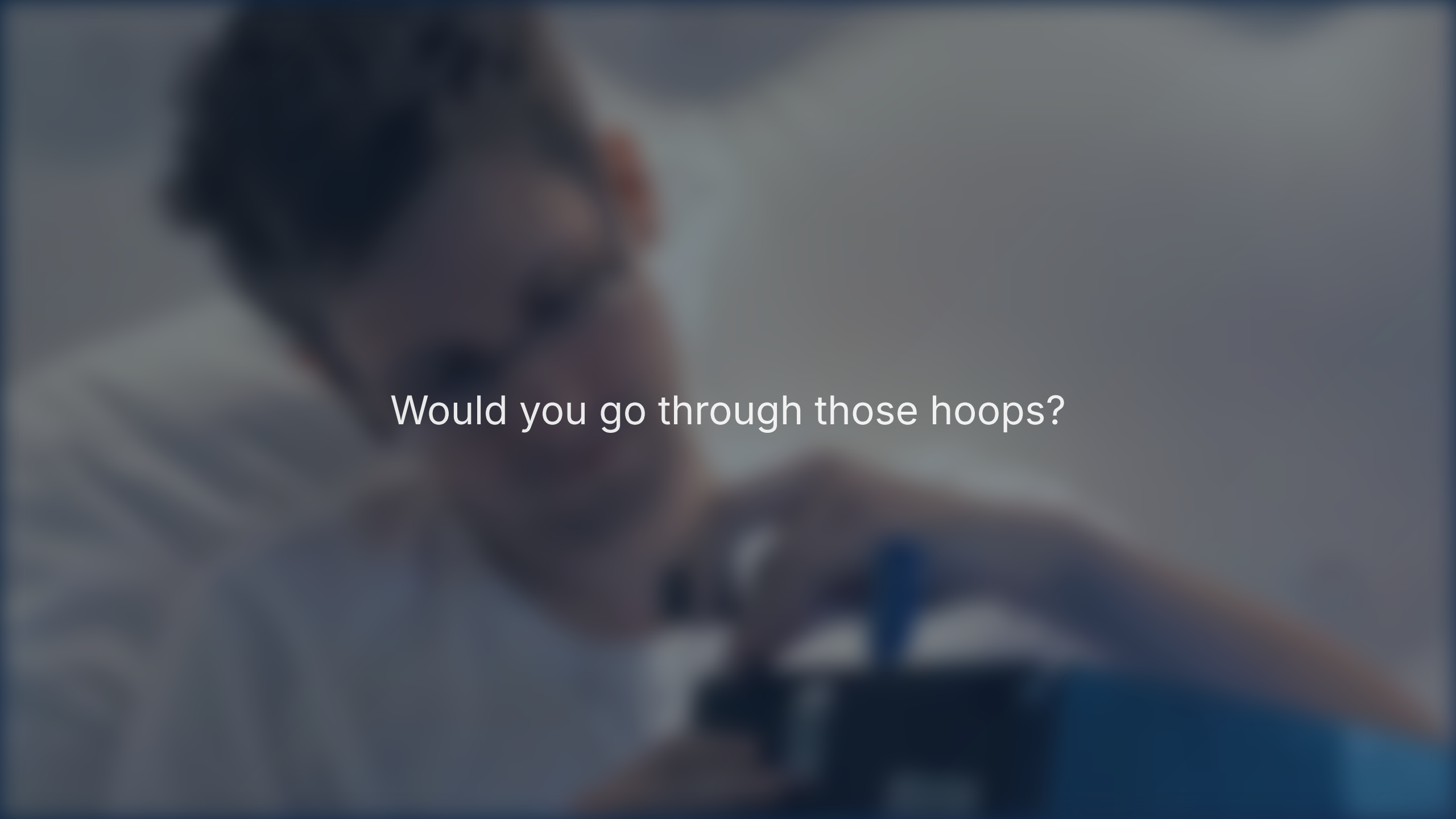
Micah Lee
@micahflee

Follow

1EBF 5F15 850C 540B 3142 F158 4BDD 496D 4C6C 5F25

11:56 PM - 28 Jan 2013

1 FAVORITE


Would you go through those hoops?

Tiplines must be advertised to everyone

Washington Post - Blended with the news articles

kill scores of civilians, monitoring group says

An Air Force mortuary chief offered to let Pentagon officials see John Glenn's body. Now it's rekindled a military scandal.

The investigation revives painful memories of a 2011 scandal that involved missing body parts, a mutilated corpse and other systemic problems.

By Craig Whitlock • 2 hours ago

House Republicans will not concede they broke a fundamental health-care promise

After a new CBO analysis finds the GOP plan would leave behind people with preexisting conditions, lawmakers seek to deflect responsibility.

By Mike DeBonis

Tillerson: U.S. takes 'full responsibility' for leaks during Manchester probe

A. Fahrenthold went in search of the missing money and found a bigger story than he ever expected.

Share news tips with us confidentially

Do you have information the public should know? Here are some ways you can securely send information and documents to Post journalists.

Learn more »

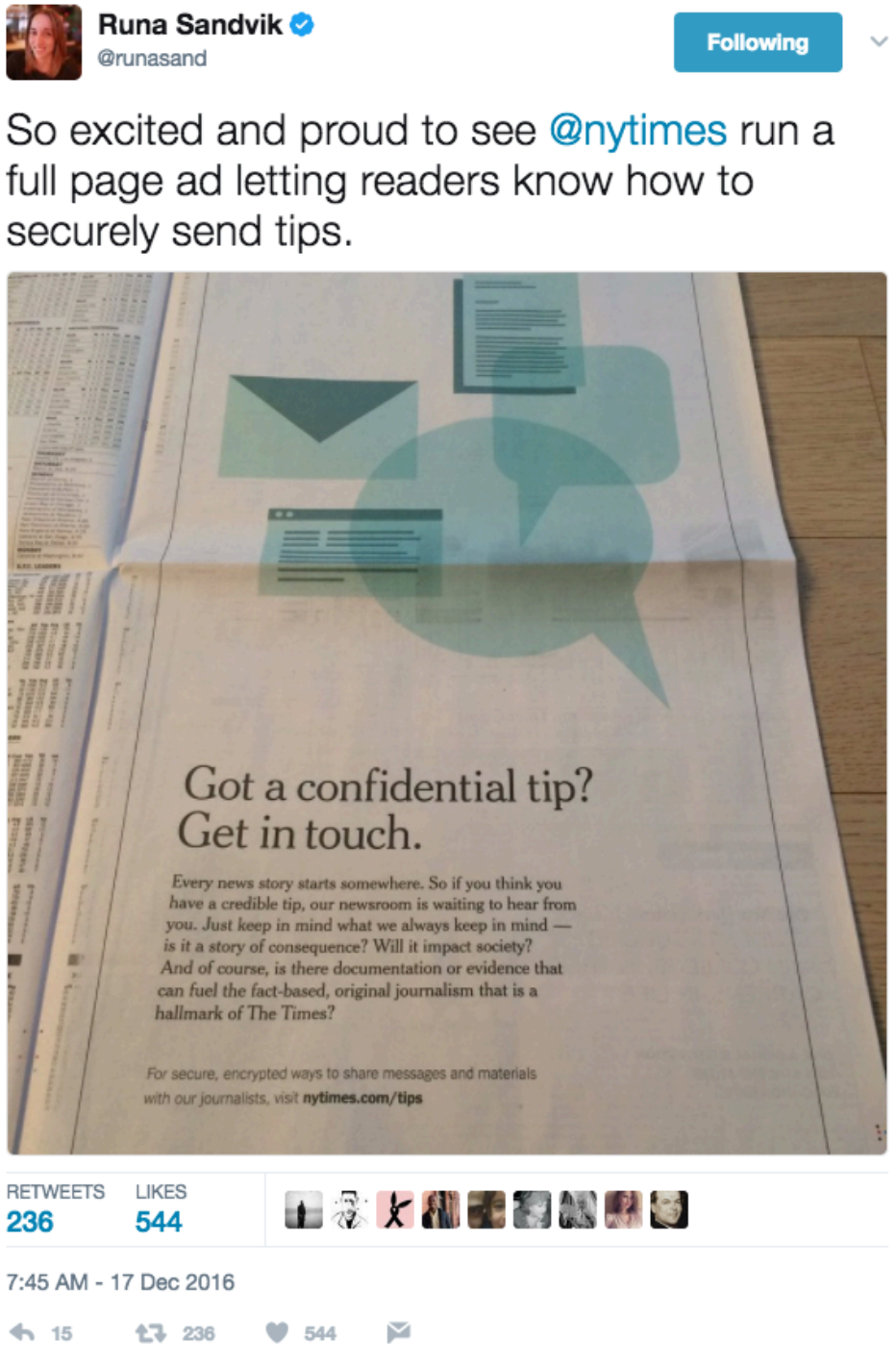
Diversions

Comics	Eggz
Crosswords	Horoscopes
Mah Jongg	Solitaire
Sudoku	TV listings

Source: Promoting Your SecureDrop Instance

Yes, even in print.

Source: Promoting Your SecureDrop Instance



The tipline landing page

What IT should know:

- **No subdomains:** use `newsroom.org/tips` not `tips.newsroom.org`
- **No analytics:** no trackers, zero logs
- **Tor-friendly** no captchas, no Javascript
- **Trustworthy hosting provider:** censorship-resistant, zero logs

The tipline landing page

What sources should know:

- **Not from work:** no corporate devices, no corporate network
- **Public spaces:** cafes, libraries, anywhere not associated with you
- **Files have fingerprints:** leaked files may get traced back to you
- **Instructions:** how to securely use Signal/SecureDrop/etc.
- **Loose lips sink ships:** never discuss whistleblowing activities

Chelsea Manning: what can go wrong

In 2010, Chelsea Manning was leaking classified documents. She felt isolated and confided in Adrian Lamo, a former "grey hat" hacker, via encrypted chat.

> *Manning wrote: "but im not a source for you ... im talking to you as someone who needs moral and emotional fucking support", and Lamo replied: "i told you, none of this is for print."*

Spoiler alert: it was.

Source: Wikipedia — Chelsea Manning

Where do we go from here?

A lot of things can go wrong. A lot of things can go right, as we learned from the now distant 2013.

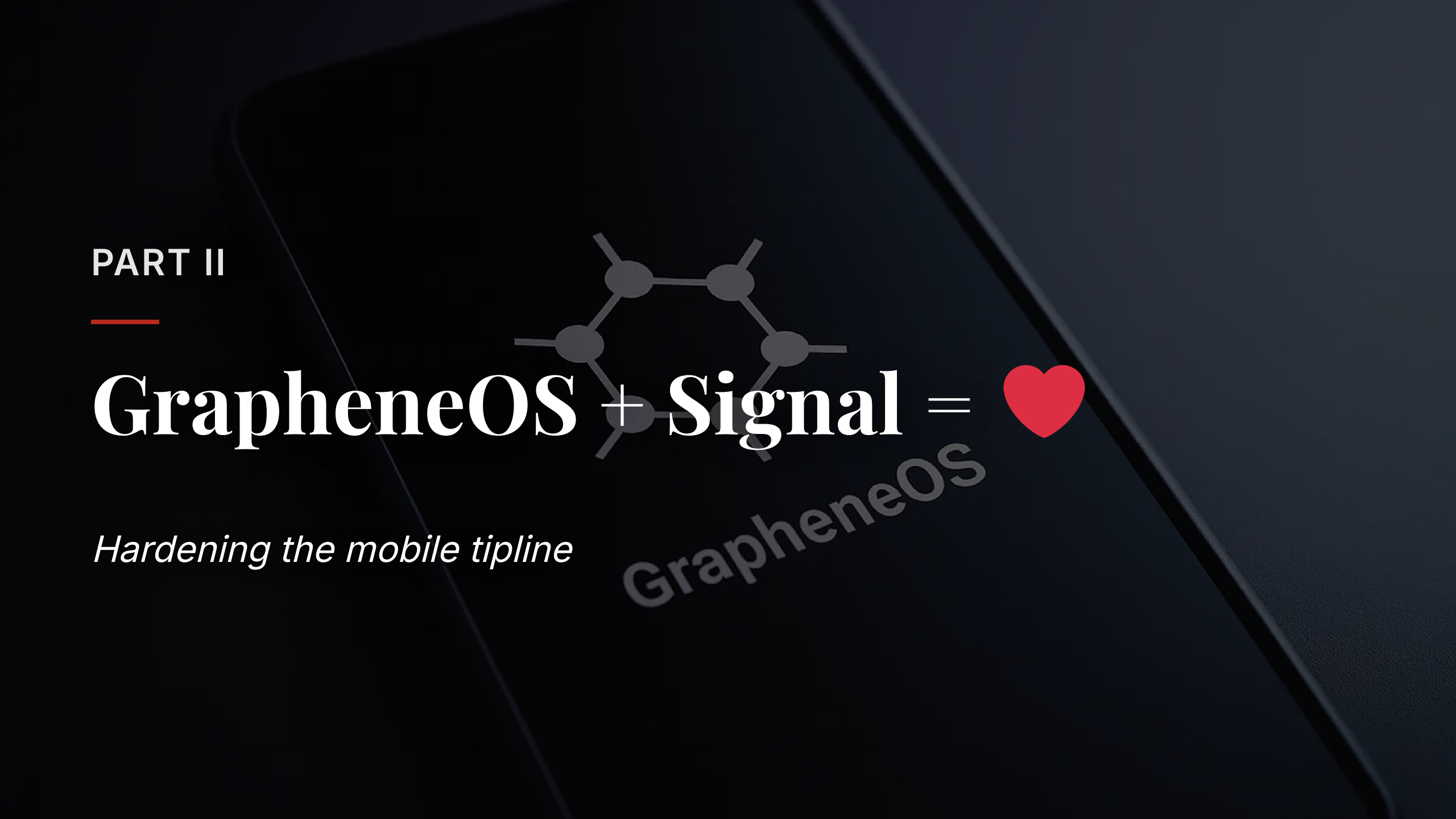
In 2026, we have new tools and more experience.

Let's go **deeper**.

PART II

GrapheneOS + Signal = ❤️

Hardening the mobile tipline



What Signal knows about you

- Signal publishes the subpoena orders that are not gagged in https://signal.org/bigbrother
- Latest subpoena shows that Signals stores very little info:

> *We received a grand jury subpoena from the United States District Court for the District of Columbia which requested customer or subscriber account information for a list of **37 phone numbers**. Specifically, it asked us to produce the **account creation date and time**, as well as the **last connection date and time** for those accounts. This showcases increasing awareness of the remarkably little information Signal can make available in response to such requests in the first place.*

Source: Signal — Grand jury subpoena for Signal user data in the United States District Court for the District of Columbia, 06 Mar 2026

What Signal knows about you

Information	How is it used	Transient?
Phone number	Used to fight spam, switch devices, discover contacts	❌
IP address	Used for rate limitting	✅
Ephemeral keys/tokens	Necessary to send messages, establish calls	✅
Registration PIN	Prevent account hijiacking	❌
Device creation date	Used when listing linked devices	❌
Last connection date	Used for device expiration logic	❌

What Signal knows about you

If Signal was forced to conduct active traffic analysis, the **IP addresses** and **ephemeral keys** *could* help law enforcement build a graph of who talks with whom.

Quick Signal wins

Setting	Why it matters
Sealed sender	Harder for Signal/AWS to track who talks with whom
Sealed sender → Allow from anyone	(see above)
Disable link previews	Previews = IP leak to the server behind the link
Registration lock	Blocks SIM-swap hijacking
~~**No notification content (iOS-only)**~~ (unnecessary as of May 2026)	Do not store incoming messages to device

Importance of Registration Lock

On January 2026, dozens of journalists became the target of a phishing attack by a fraudulent "Signal Security Support ChatBot" account:

> *Dear User, this is Signal Security Support ChatBot. We have noticed suspicious activity on your device, which could have led to data leak. We have also detected attempts to gain access to your private data in Signal. To prevent this, you have to pass verification procedure, entering the verification code to Signal Security Support Chatbot. DON'T TELL ANYONE THE CODE, NOT EVEN SIGNAL EMPLOYEES.*

Possible end goal:

- Reveal who communicates with whom.
- Read messages **after** takeover.

Source: Netzpolitik — Numerous journalists targeted in attack via Signal Messenger

What about the device itself?

On January 2026 (again!) the FBI **raided** the home of Washington Post reporter Hannah Natanson, to gain access to her Signal contacts, which included at least **1,169** former and present US federal employees.

Here's what we know from a court order:

> *[...] Because the iPhone was in Lockdown mode, CART could not extract that device*

Source: 404 Media — FBI Couldn't Get into WaPo Reporter's iPhone Because It Had Lockdown Mode Enabled

How Cellebrite and others work

Important terms:

- **BFU** (Before First unlock)
  Device powered off or just booted
- **AFU** (After First unlock)
  Device has been unlocked at least once
- **TPM** (Trusted Platform Module)
  Onboard-chip that prevents PIN guessing
  - Available on iOS and certain Android devices.

Table 3: Android OS Access Support Matrix – Google Pixel 7.75.3

Model / State	Standard Android OS, BFU	Standard Android OS, AFU	Standard Android OS, Unlocked	GrapheneOS, BFU *	GrapheneOS, AFU *	GrapheneOS, Unlocked
Pixel 6 / Pixel 6 Pro / Pixel 6a	BFU Yes BF No	FFS Yes BF No	FFS Yes	BFU Yes, up to late 2022 SPL BF No	FFS Yes, up to late 2022 SPL BF No	FFS Yes, up to late 2024 SPL
Pixel 7 / Pixel 7 Pro / Pixel Ta / Pixel Tablet / Pixel Fold	BFU Yes BF No	FFS Yes BF No	FFS Yes	BFU Yes, up to late 2022 SPL BF No	FFS Yes, up to late 2022 SPL BF No	FFS Yes, up to late 2024 SPL
Pixel 8 / Pixel 8a / Pixel 8 Pro	BFU Yes BF No	FFS Yes BF No	FFS Yes	BFU Yes, up to late 2022 SPL BF No	FFS Yes, up to late 2022 SPL BF No	FFS Yes, up to late 2024 SPL
Pixel 9 / Pixel 9 Pro / Pixel 9 Pro XL / Pixel 9 Pro Fold / Pixel 9a	BFU Yes BF No	FFS Yes BF No	FFS Yes	BFU No BF No	FFS No BF No	FFS Yes, up to late 2024 SPL

Source: GrapheneOS Discussion Forum: New Cellebrite capability obtained in Teams meeting
Date: October 29, 2025

Cat and mouse game

- Lagging a bit behind iOS / Pixel releases
- Android devices without TPM can be trivially extracted
- BFU (passphrase) > BFU (PIN) > AFU
- GrapheneOS has a section of its own and no serious exploit

Quick phone wins

Setting	Why it matters
Lockdown mode (iOS)	Protection against device seizures/spyware
Advanced Protection (Android)	Protection against device seizures/spyware
No SIM card (newsroom devices)	lots of 0-days target SMS/MMS

GrapheneOS

Setting	Why it matters
Auto-reboot	Brings device to BFU if not unlocked for `N` hours
Disable USB port on lock screen	Prevents software bugs
Sandboxed Google Play	Makes Google integration smaller
User profiles	Different settings/passwords/apps per profile
Hardware attestation	Protection against evil-maid attacks
Duress password	Wipe device in case of physical intimidation

Live demo: GrapheneOS + Signal

- Simple installation
- User profiles (personal, tips, vaults)
- Receiving a tip via Signal
- Device VPN (Orbot)
- Secure PDF viewer / browser

PART III

Perimeter security

Walls have ears, we have gears.

PART IV

QubesOS + SecureDrop = ❤️

Compartmentalization as a defense.

Remember that WaPo reporter?

FBI also seized her Macbook, portable hard drive and audio recording device

and a cell phone upstairs and that she did not use biometrics on her devices. *See id.* In the upstairs of the house, investigators located a powered-off silver MacBook Pro with a black case, an Apple iPhone 13, a Handy branded audio recording device, and a Seagate portable hard drive. *See id.* ¶ 26. Investigators seized these devices. The iPhone was found powered on and charging, and its display noted that the phone was in "Lockdown" mode. *See id.* ¶ 27. Investigators also seized

… and gained access to it

necessary to determine whether that data falls within the items to be seized." *Id.* The warrant further authorized investigators to "press or swipe" Ms. Natanson's fingers "to the fingerprint scanner of the device" and to "hold a device found during the search in front of [her] face" to activate any facial recognition feature "for the purpose of attempting to unlock" that particular device. *Id.* at 7.

Source: Freedom of the Press Foundation — Five security lessons from the FBI's Washington Post raid

Remember that WaPo reporter?

Then they took pictures and video recordings of the conversations and the attachments, because they noticed "Disappearing messages" were turned on.

id. ¶ 41. Investigators noticed that several of Ms. Natanson's Signal chat messages were set for auto-deletion. *See id.* ¶ 40. Agents thus worked in a reverse chronological order to take pictures of the Signal conversations for only those conversations in which the display date of the last message, attachment, notification, conversation setting change, etc. was on or after October 1, 2025, consistent with Attachment B. *See id.* ¶ 45. Once the conversations were photographed in their entirety, as they appeared on screen, agents then attempted to manually click on and open every attachment and file contained within each conversation, again solely to preserve the information. *See id.* ¶ 47. For audio messages that they discovered, investigators captured those

Source: Freedom of the Press Foundation — Five security lessons from the FBI's Washington Post raid

Possible outcomes

- The FBI knows the display names / avatars of her Signal sources.
- They can work in reverse and subpoena Signal to give them the phone numbers.
  - We are not aware of any such action yet.

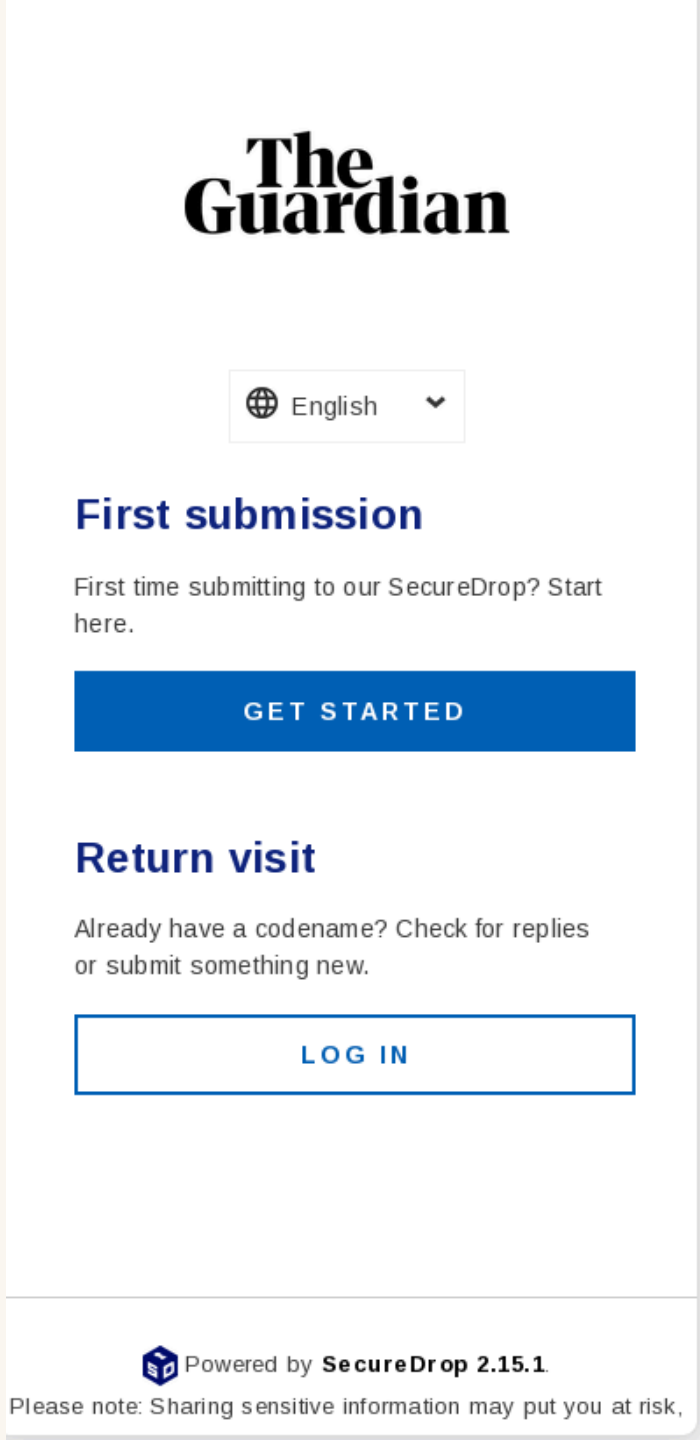
Signal has managed to wrangle source confidentiality and ease of use **extremely well**.

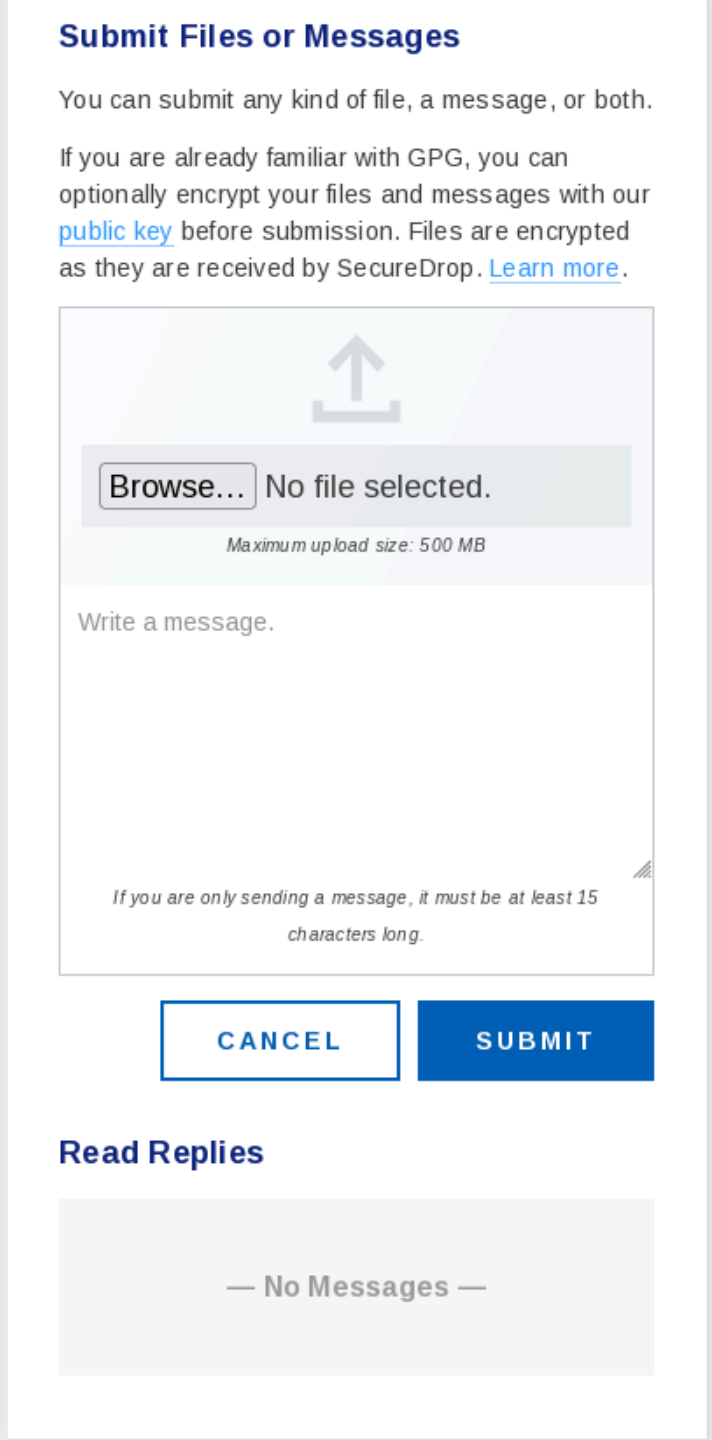
Sources with a different threat model may choose to use SecureDrop.

And that's a much different beast...

SecureDrop overview - Sources

- Sources visit Tor site, receive a long codename.
- Sources can send messages, attachments.
- Sources can learn about replies only if they visit again.

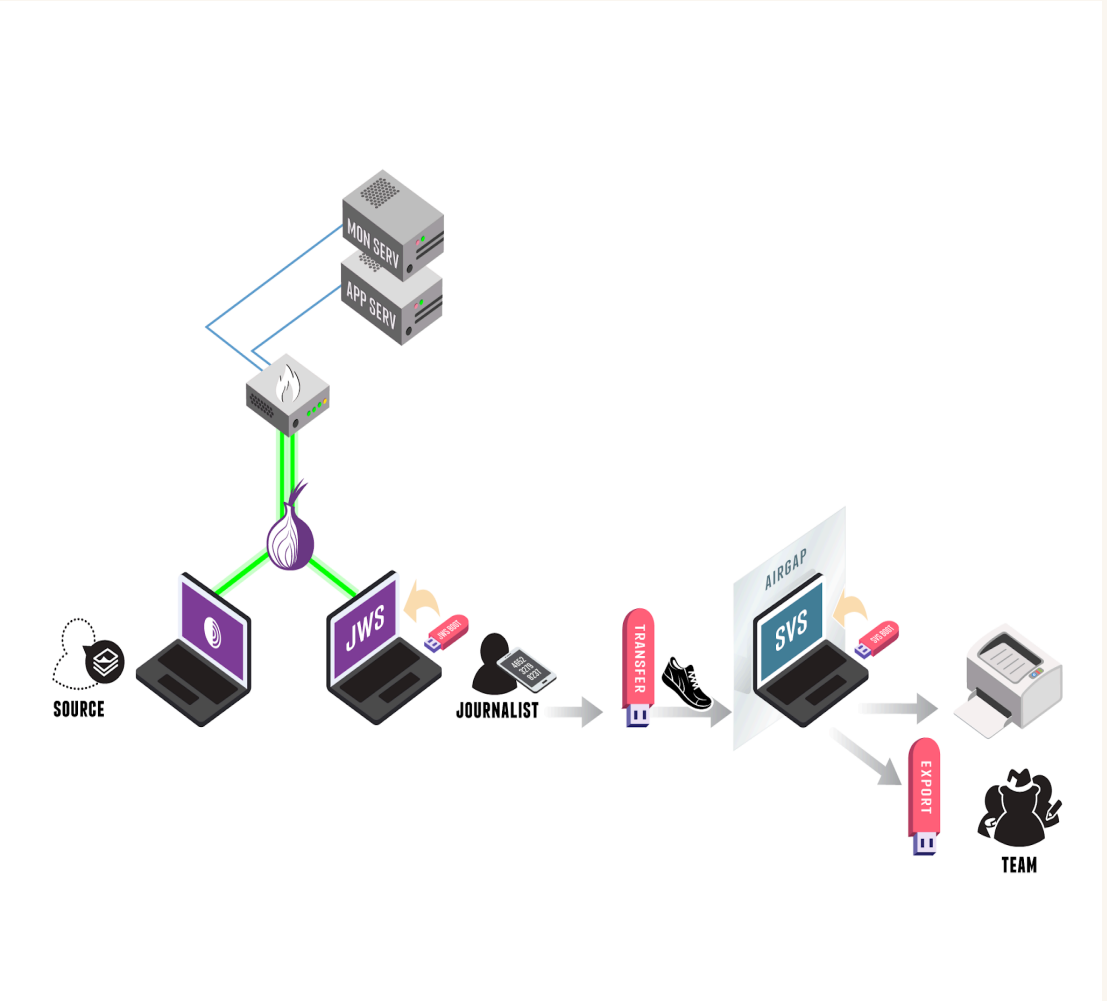




SecureDrop overview - Journalists

Journalists have two laptops and four USB keys.

Realistically, interacting with submissions takes **a lot** of time.

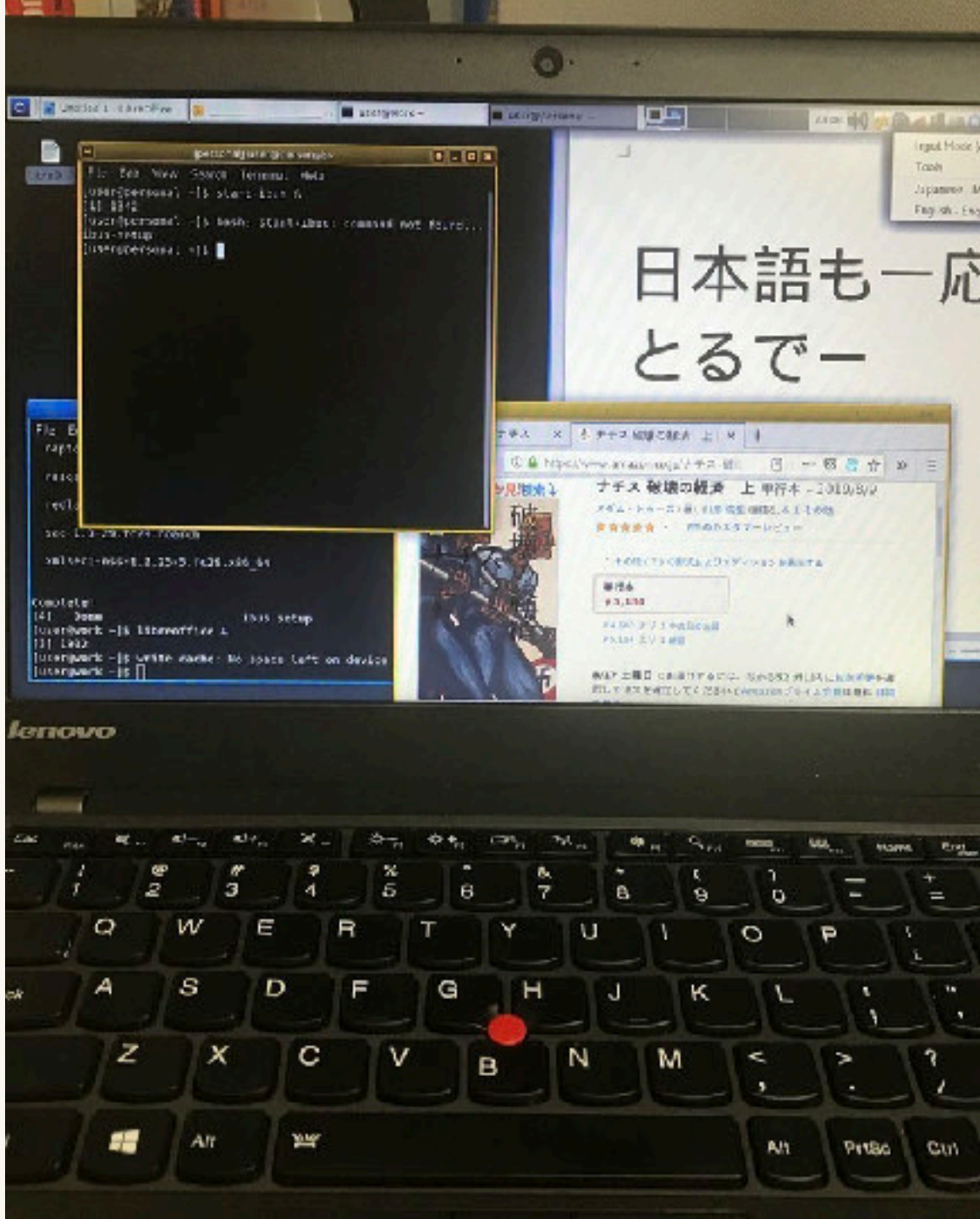


Can we have a single laptop please?

Qubes OS

- Linux-based OS
- Same target group as Tails
- ... but everything is a VM
- Different window colors per environment
- Not a daily driver, but a special-purpose machine

No need for different Tails keys!



Live Demo: QubesOS + SecureDrop

- Personal, work, vault environments
- Safe file viewing and printing
- Search messages, export transcripts

PART V

Post-verification

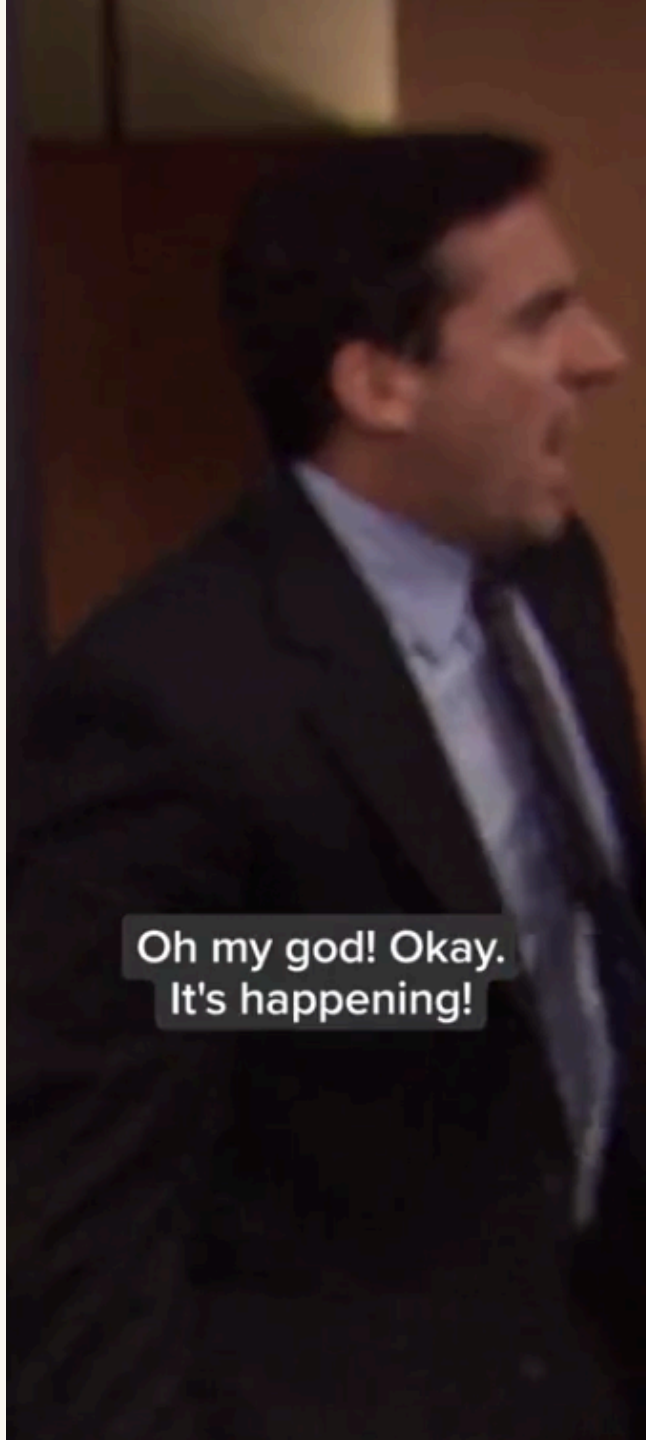
Store it, share it, publish it, without burning your source.

Post-verification

You have verified in a secure fashion that the material is important.

Possible scenarios:

- **Store it**
- **Share it privately**
- **Go public**



Store it offline

Use Veracrypt on any USB drive!

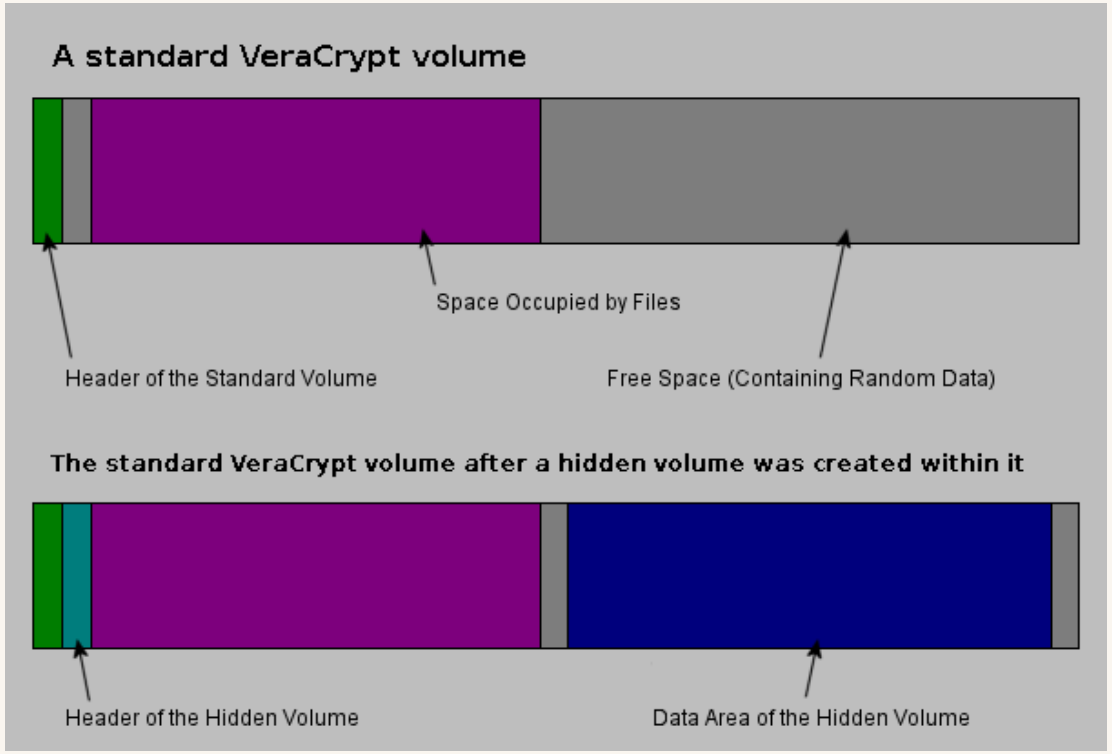
- Available on Windows/macOS
- Third-party support on Android/iOS
- Open-source
- Offers plausible deniability

Plausible deniability

A Veracrypt drive can consist of two volumes:

- **Outer volume:** Place decoy files in there (tax / health records, previous investigations).
- **Inner (hidden) volume:** Place sensitive files in there.

In duress, offer the password of the **outer volume**.



Making it tamper-evident

In cases of:

- Shipping USB drive to someone
- Crossing borders
- Long-term storage

(TS//SI//NF) Such operations involving **supply-chain interdiction** are some of the most productive operations in TAO, because they pre-position access points into hard target networks around the world.

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

Source: dys2p.com — Random Mosaic – Detecting unauthorized physical access with beans, lentils and colored rice

Sender's Name MICAH LEE Phone [redacted]

Company

Address [redacted]

Address

City BERKELEY State Province CA

Country UNITED STATES ZIP Postal Code [redacted]

2 To

Recipient's Name GLENN GREENWALD Phone

Company

Address [redacted]

Dept./Floor

Address [redacted]

City RIO DE JANEIRO State Province

Country BRAZIL ZIP Postal Code [redacted]

Recipient's Tax ID Number for Customs Purposes
e.g., GST/RFC/VAT/IVE/NAB, or as locally required.

3 Shipment Information ☐ For EU Only: Tick here if goods are not in free circulation and provide C.I.

Total Packages (Shipper's Load and Count/SLAC) Total Weight ☐ lbs. ☐ kg DIM L / W / H ☐ in. ☐ cm

Commodity Description	Harmonized Code	Country of Manufacture	Value for Customs
FLASH DRIVE GIFT		USA	$10

☐ FedEx Intl. Economy
FedEx Envelope and FedEx Pak rate not available.

5 Packaging *These unique brown boxes with special pricing are provided by FedEx for FedEx Intl. Priority only.

☑ FedEx Envelope ☐ FedEx Pak ☐ FedEx Box ☐ FedEx Tube
☐ Other ☐ FedEx 10kg Box* ☐ FedEx 25kg Box*

6 Special Handling

☐ HOLD at FedEx Location ☐ SATURDAY Delivery
Available to select locations for FedEx Intl. Priority only.

7 Payment Complete payment options for both transportation charges and duties and taxes.

Bill transportation charges to: Enter FedEx Acct. No. or Credit Card No. below.

☐ Sender Acct. No. in Section 1 will be billed ☐ Recipient ☐ Third Party ☑ Credit Card ☐ Cash Check/Cheque

FedEx Use Only

FedEx Acct. No.

Credit Card No.

Credit Card Exp. Date

Bill duties and taxes to: ALL shipments may be subject to Customs charges, which FedEx does not estimate prior to clearance.

Enter FedEx Acct. No. below.

☐ Sender Acct. No. in Section 1 will be billed ☑ Recipient ☐ Third Party

FedEx Acct. No.

8 Your Internal Billing Reference First 24 characters will appear on invoice.

OPTIONAL

9 Required Signature

Use of this Air Waybill constitutes your agreement to the Conditions of Contract on the back of this Air Waybill, and you represent that this shipment does not require a U.S. State Department License or contain dangerous goods. Certain international treaties, including the Warsaw Convention, may apply to this shipment and limit our liability for damage, loss, or delay, as described in the Conditions of Contract. **WARNING:** These commodities, technology, or software were exported from the United States in accordance with Export Administration Regulations. Diversion contrary to U.S. law prohibited.

Sender's Signature: Micah Lee

This is not authorization to deliver this shipment without a recipient signature.

For Completion Instructions, see back of fifth page.

FedEx Tracking Number 8026 7146 [redacted]

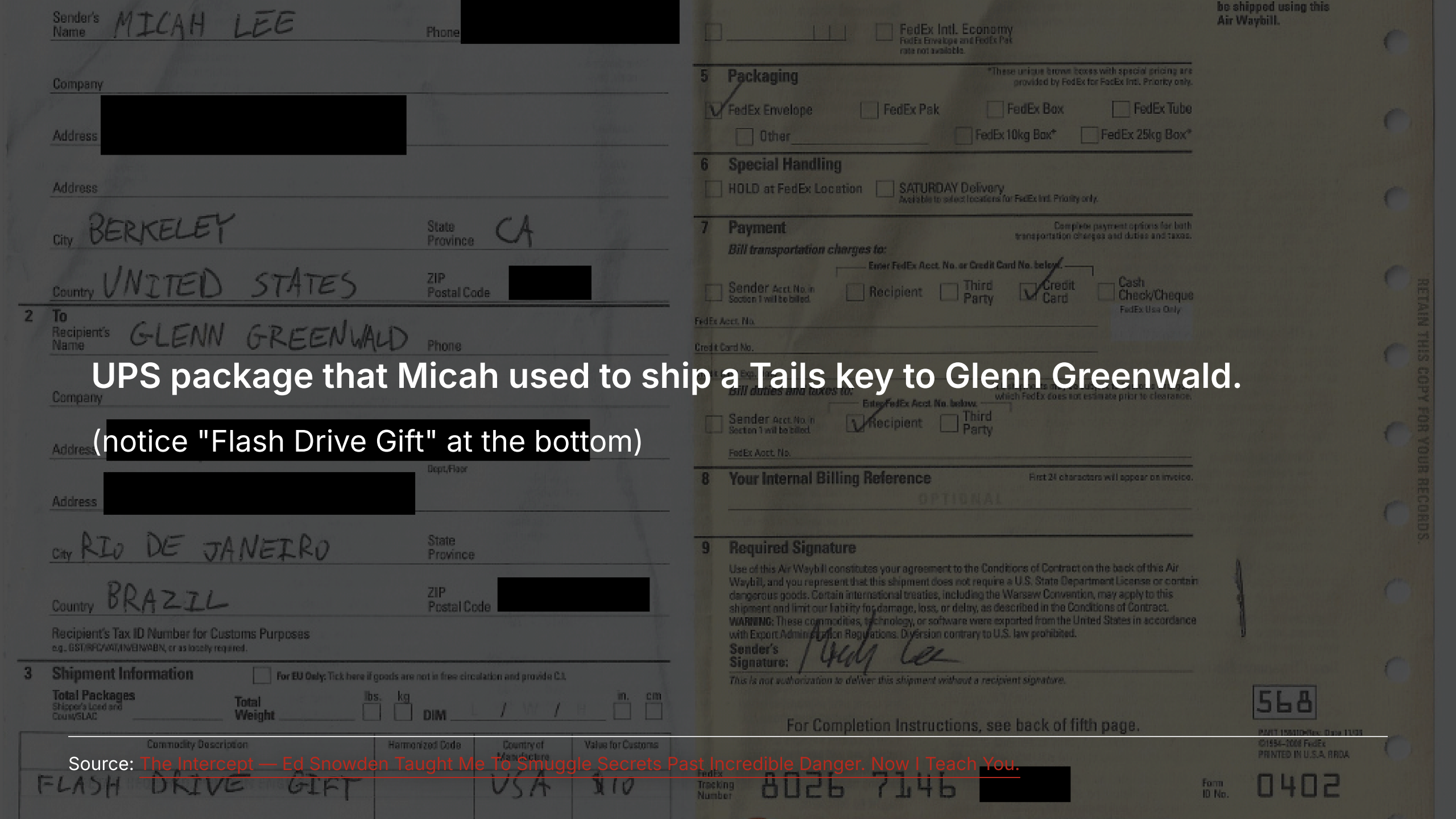
Form ID No. 0402

568

PART 15841D•Rev. Date 11/08
©1994–2008 FedEx
PRINTED IN U.S.A. RRDA

be shipped using this Air Waybill.

RETAIN THIS COPY FOR YOUR RECORDS.



UPS package that Micah used to ship a Tails key to Glenn Greenwald.

(notice "Flash Drive Gift" at the bottom)

Source: The Intercept — Ed Snowden Taught Me To Smuggle Secrets Past Incredible Danger. Now I Teach You.

Making it tamper-evident (the boring way)

One way is to buy tamper evident bags...

... but if your threat model is law enforcement, assume that they have ways around it.

(here, it's just a syringe with acetone)

Source: DEF CON 30 - Tamper Evident Village

Making it tamper-evident (the fun way)

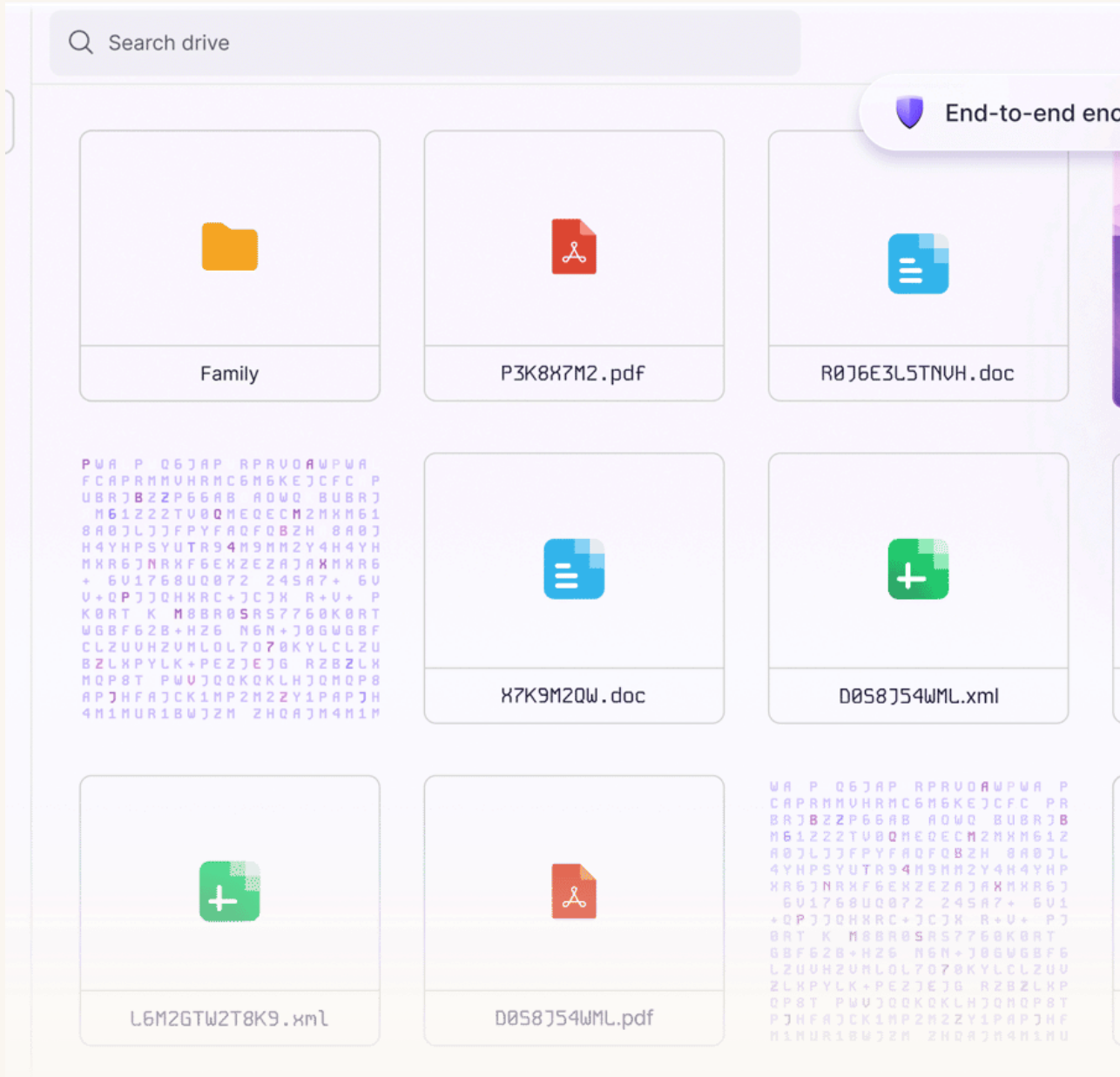
1. Grab a bean mix
2. Wrap the USB drive with plastic wrap
3. Put the beans and the USB drive in a vacuum bag
4. Seal it with a vacuum sealer
5. Take a picture of it from both sides
6. Verify the mosaic with BlinkComparison (Android-only)

Showcase of how blink comparison works

Source: dys2p.com — Random Mosaic – Detecting unauthorized physical access with beans, lentils and colored rice

Store it online

- Proton Drive offers end-to-end encryption.
- For the paranoid, you can even create an anonymous account using Tor.

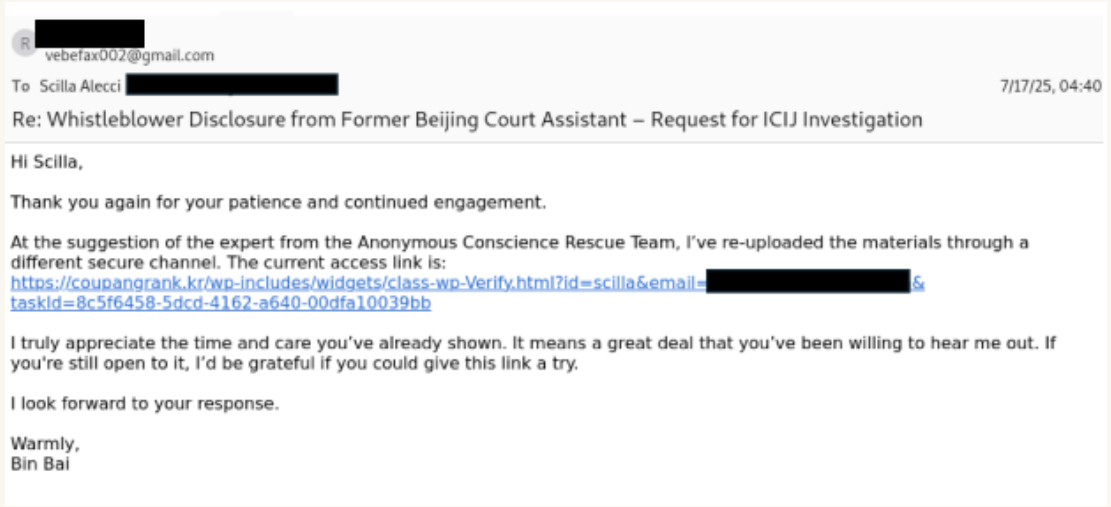


Sharing it privately

- Anonymous tips cannot always be trusted.
- The fact that you opened it in QubesOS /GrapheneOS safely does not mean others have the same system.
- Files must be sanitized.

Phony whistleblowers

The lure of confidential info was used against ICIJ journalists since April 2025 by Chinese state actors pretending to be whistleblowers:



[redacted]
vebefax002@gmail.com

To Scilla Alecci [redacted] 7/17/25, 04:40

Re: Whistleblower Disclosure from Former Beijing Court Assistant – Request for ICIJ Investigation

Hi Scilla,

Thank you again for your patience and continued engagement.

At the suggestion of the expert from the Anonymous Conscience Rescue Team, I've re-uploaded the materials through a different secure channel. The current access link is:
https://coupangrank.kr/wp-includes/widgets/class-wp-Verify.html?id=scilla&email=[redacted]&
taskId=8c5f6458-5dcd-4162-a640-00dfa10039bb

I truly appreciate the time and care you've already shown. It means a great deal that you've been willing to hear me out. If you're still open to it, I'd be grateful if you could give this link a try.

I look forward to your response.

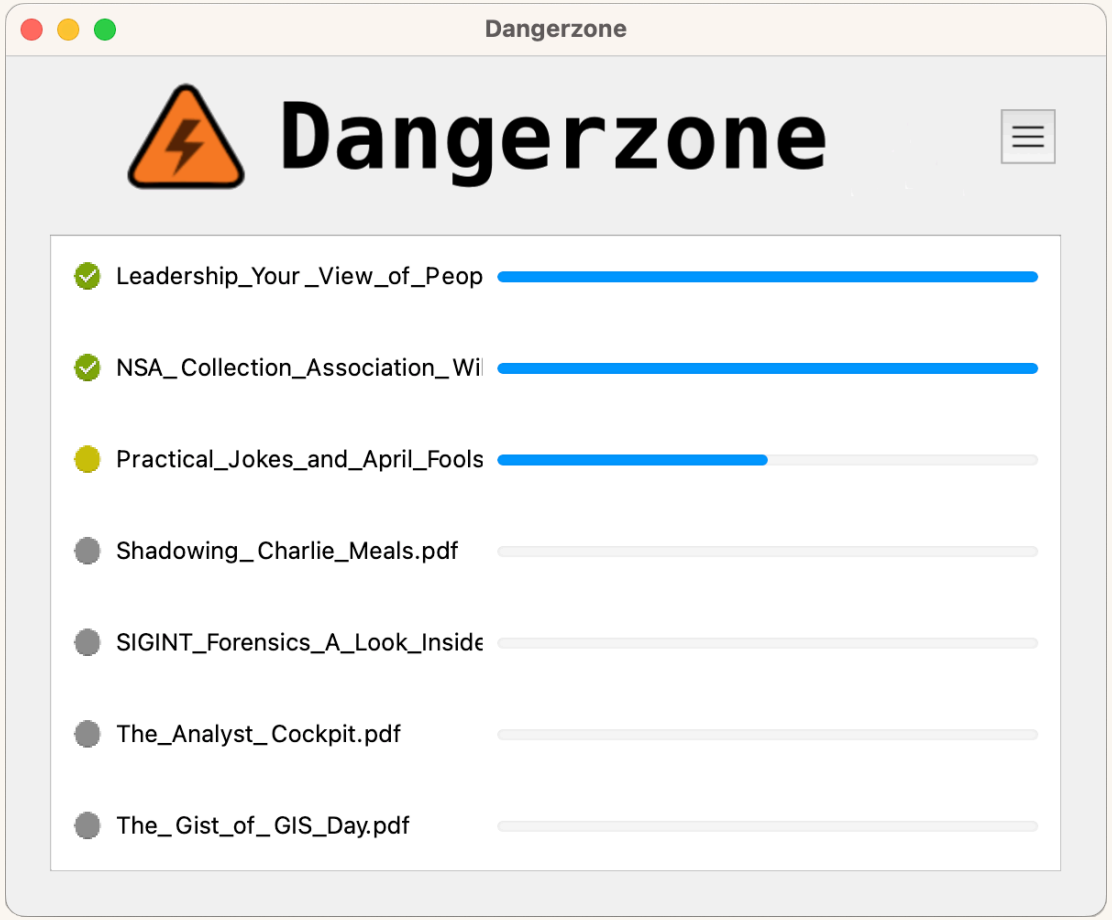
Warmly,
Bin Bai

> *The email included a link that "Bai" said led to an **archive full of confidential records**. ICIJ concluded that the link was likely **malicious**, the **whistleblower a fake**, and the email a clumsy attempt to steal the reporter's login details to access **source information and other sensitive data**.*

Source (left): The Citizen Lab — How Chinese Actors Use Impersonation and Stolen Narratives to Perpetuate Digital Transnational Repression
Source (right): ICIJ — Phony whistleblowers, fake journalists and cyber spies: ICIJ network targeted after China Targets probe

Dangerzone

- Open source desktop app
- Maintained by Freedom of the Press Foundation
- Supports Windows, macOS, Linux, Tails, Qubes
- Supports more than 20 file types (PDFs, office, images)
- https://dangerzone.rocks

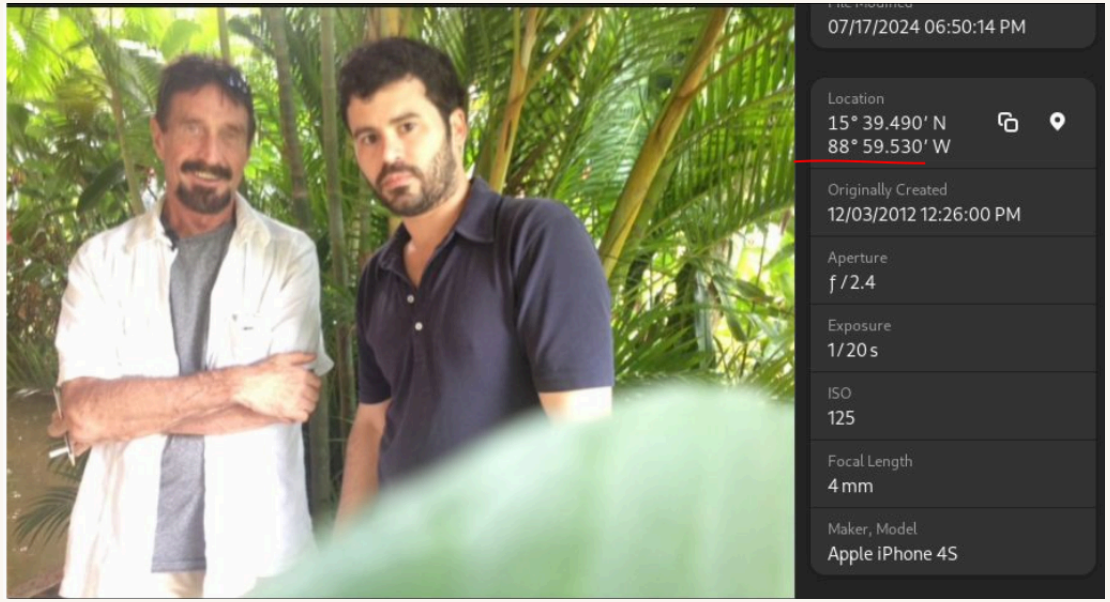


Going public

The material may have de-anonymization vectors that point back to the source.

Let's see some prominent examples.

Exhibit A - Simple metadata (multimedia)



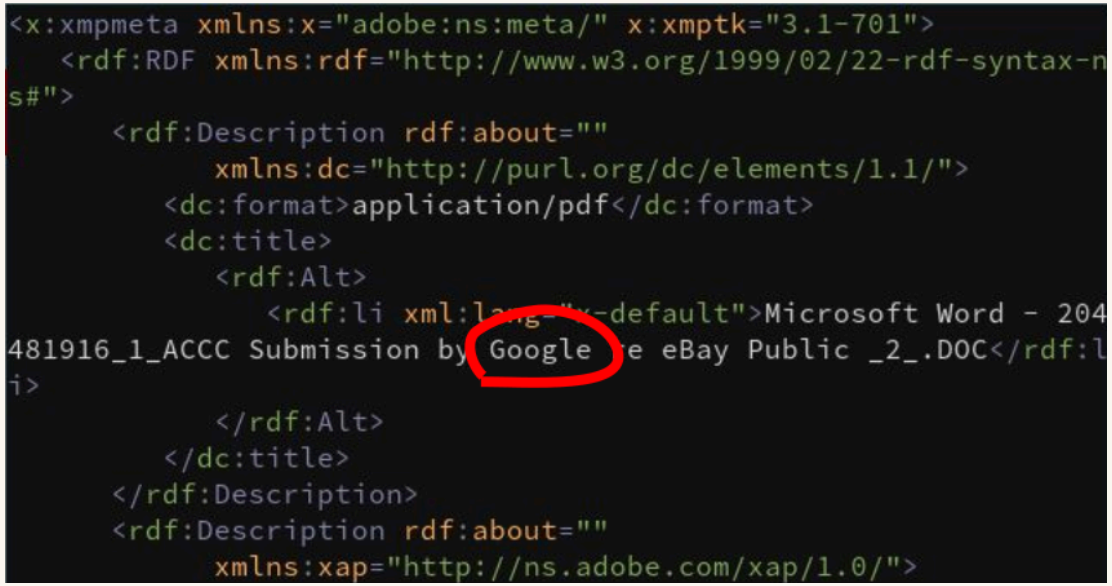
WIRED

Oops! Did Vice Just Give Away John McAfee's Location With Photo Metadata?

⚠️Photos may contain location and author info

Source: Wired — Oops! Did Vice Just Give Away John McAfee's Location With Photo Metadata?

Exhibit B - Complex metadata (PDF, MS Office)



```
<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="3.1-701">
   <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-n
s#">
      <rdf:Description rdf:about=""
            xmlns:dc="http://purl.org/dc/elements/1.1/">
         <dc:format>application/pdf</dc:format>
         <dc:title>
            <rdf:Alt>
               <rdf:li xml:la[illegible]-default">Microsoft Word - 204
481916_1_ACCC Submission by Google [illegible]e eBay Public _2_.DOC</rdf:l
i>
            </rdf:Alt>
         </dc:title>
      </rdf:Description>
      <rdf:Description rdf:about=""
            xmlns:xap="http://ns.adobe.com/xap/1.0/">
```

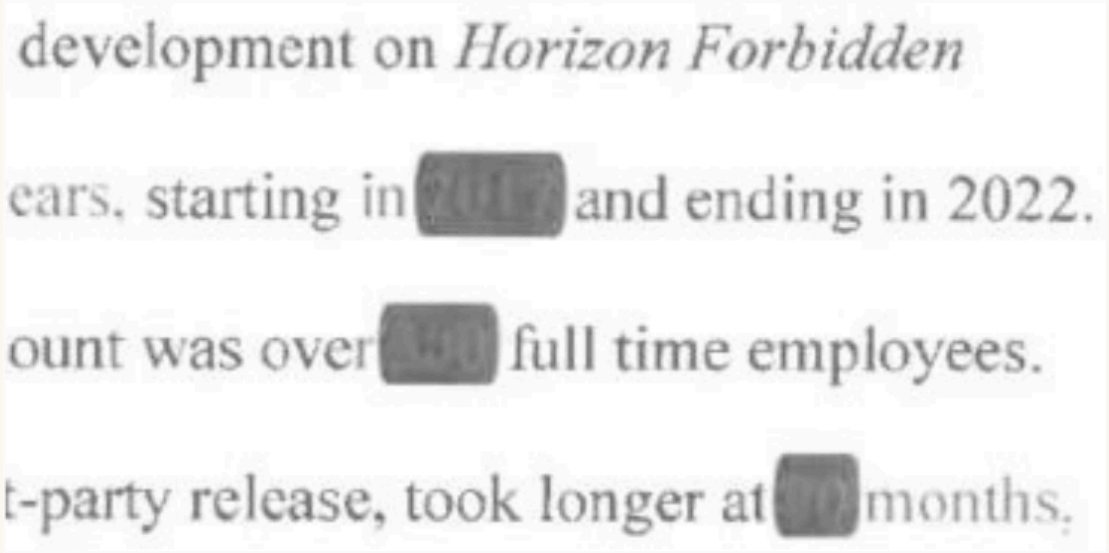
The Register

Metadata ruins Google's anonymous eBay Australia protest

⚠️ PDFs and office documents may contain nested metadata.
Think embedded photos, Word's tracking changes feature.

Source: The Register — Metadata ruins Google's anonymous eBay Australia protest

Exhibit C - Redactions


development on *Horizon Forbidden*

ears, starting in [redacted] and ending in 2022.

ount was over [redacted] full time employees.

t-party release, took longer at [redacted] months.

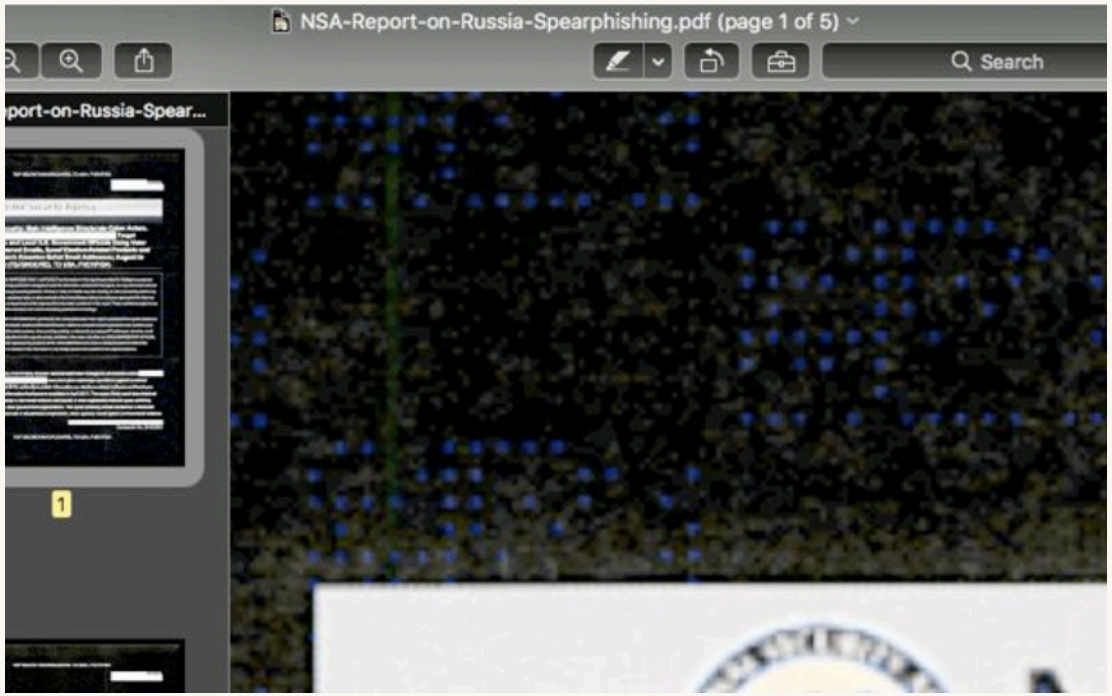
The Verge

Sony's confidential PlayStation secrets just spilled because of a Sharpie / The black Sharpie strikes again to reveal Sony's Call of Duty revenue secrets.

⚠️ Redactions do not work if in a layer or not opaque

Source: The Verge — Sony's confidential PlayStation secrets just spilled because of a Sharpie

Exhibit D - Physical watermarks



The Atlantic

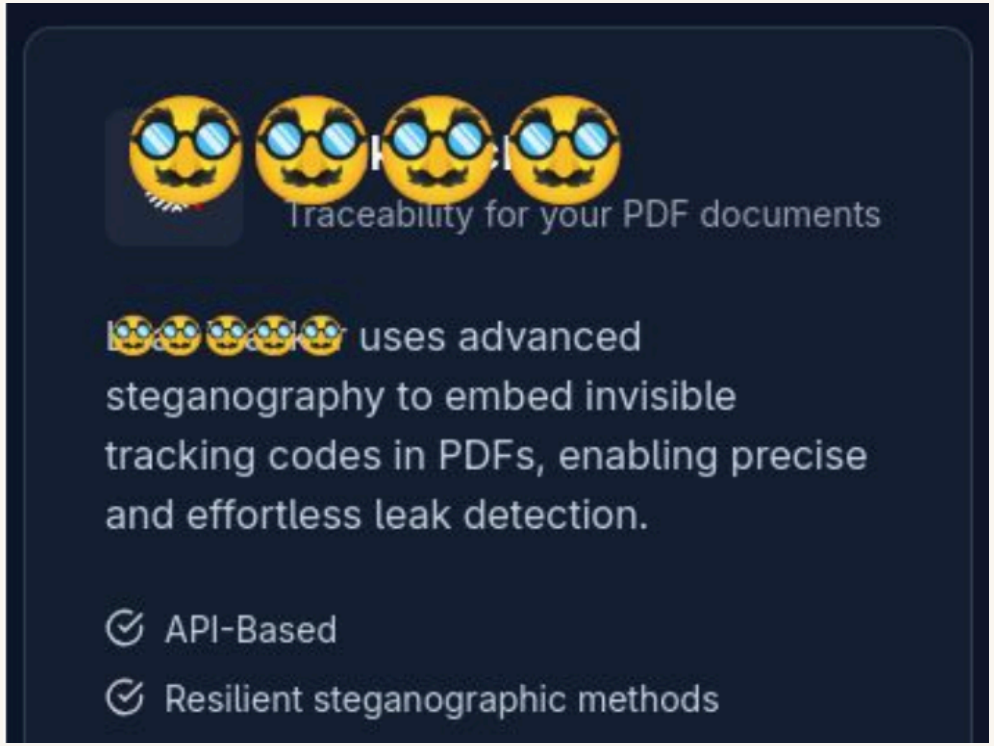
The Mysterious Printer Code That Could Have Led the FBI to Reality Winner

Many color printers embed grids of dots that allow law enforcement to track every document they output.

⚠️ Printed documents may contain tracking dots

Source: The Atlantic — The Mysterious Printer Code That Could Have Led the FBI to Reality Winner

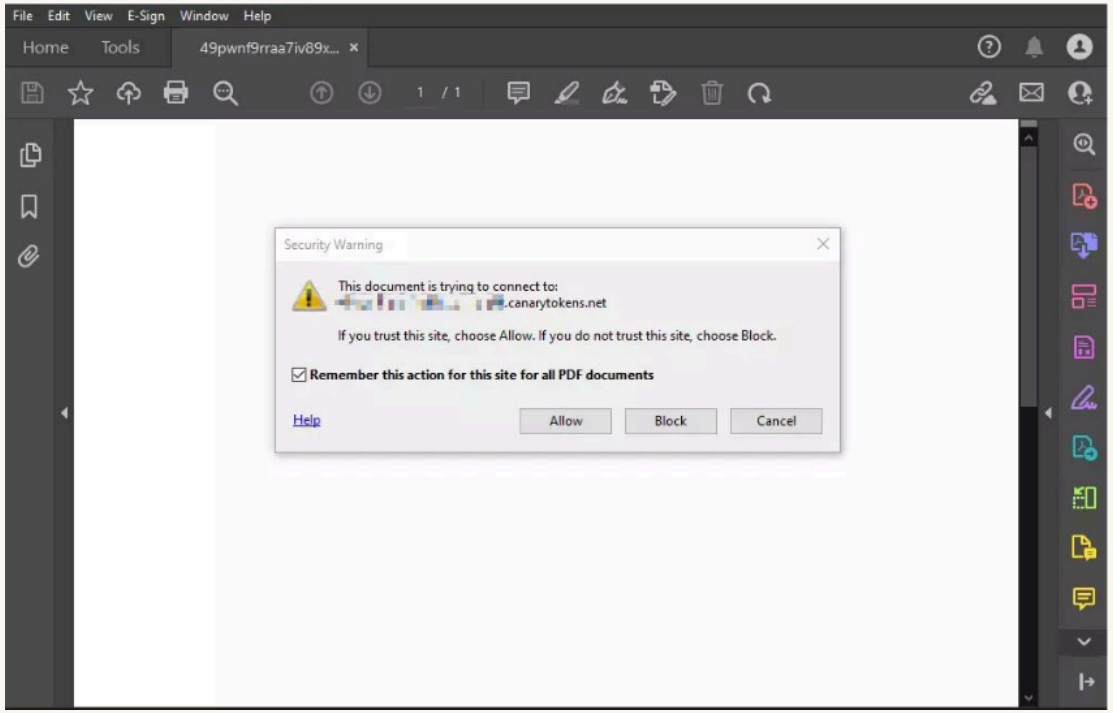
Exhibit E - Digital watermarks



⚠️ Digital material accessible only to you may have invisible watermarks

Source: The Intercept — How Elon Musk Says He Catches Leakers at His Companies

Exhibit F - Canary tokens

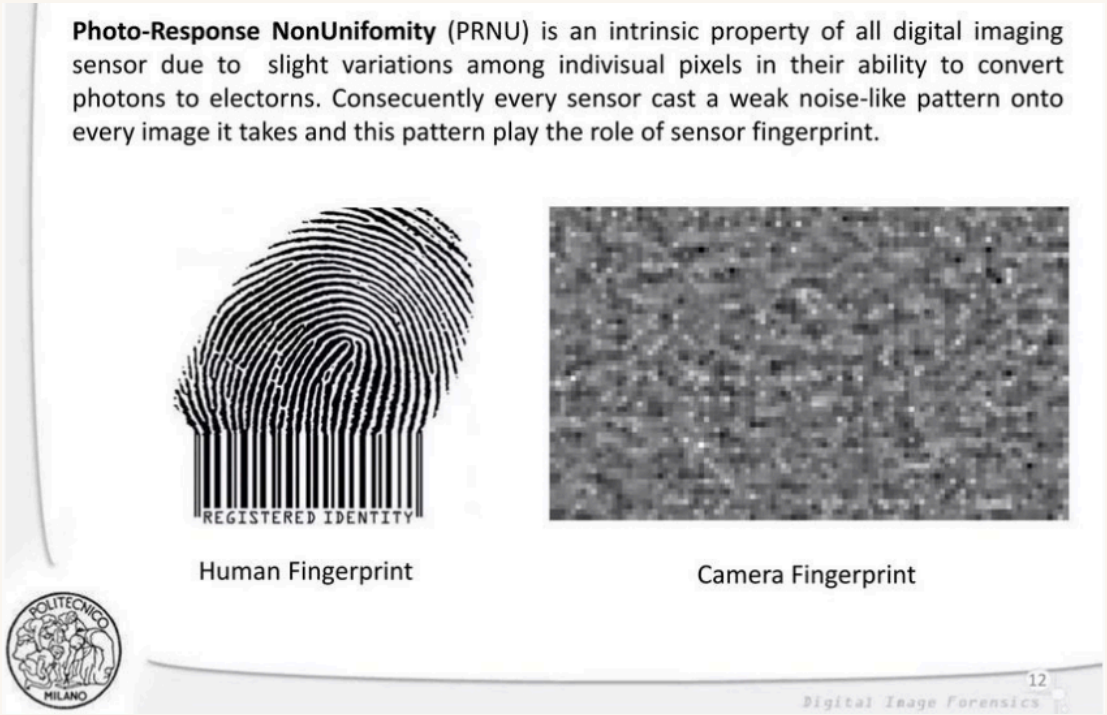


- Most sane document viewers block them silently.
- Microsoft Office asks to enable macros.
- Adobe Acrobat asks if it's ok to connect to site.
- Deanonymization is a click away.

⚠️ Trapped documents may phone home in major viewers

Source: Austin Martin — Canary Tokens

Exhibit G - Fingerprinting



- Cameras, mics are subject to fingerprinting
- Your way of writing is a fingerprint (stylometry)
- Unlike watermarking, fingerprinting is useful only with a second match (much like human fingerprints)

⚠️ A/V equipment and writing style can be fingerprinted

Source: Digital Image Forensics: Camera Fingerprint and its Robustness

Exhibit H - Environment

Japanese “Sasaeng” Tracked down a Female Idol’s Home by Zooming in on the Reflection in Her Eyes

⚠️ Cameras, microphones capture the surrounding environment

Source: Koreaboo — Japanese “Sasaeng” Tracked down a Female Idol’s Home by Zooming in on the Reflection in Her Eyes

Going public

Practical advice:

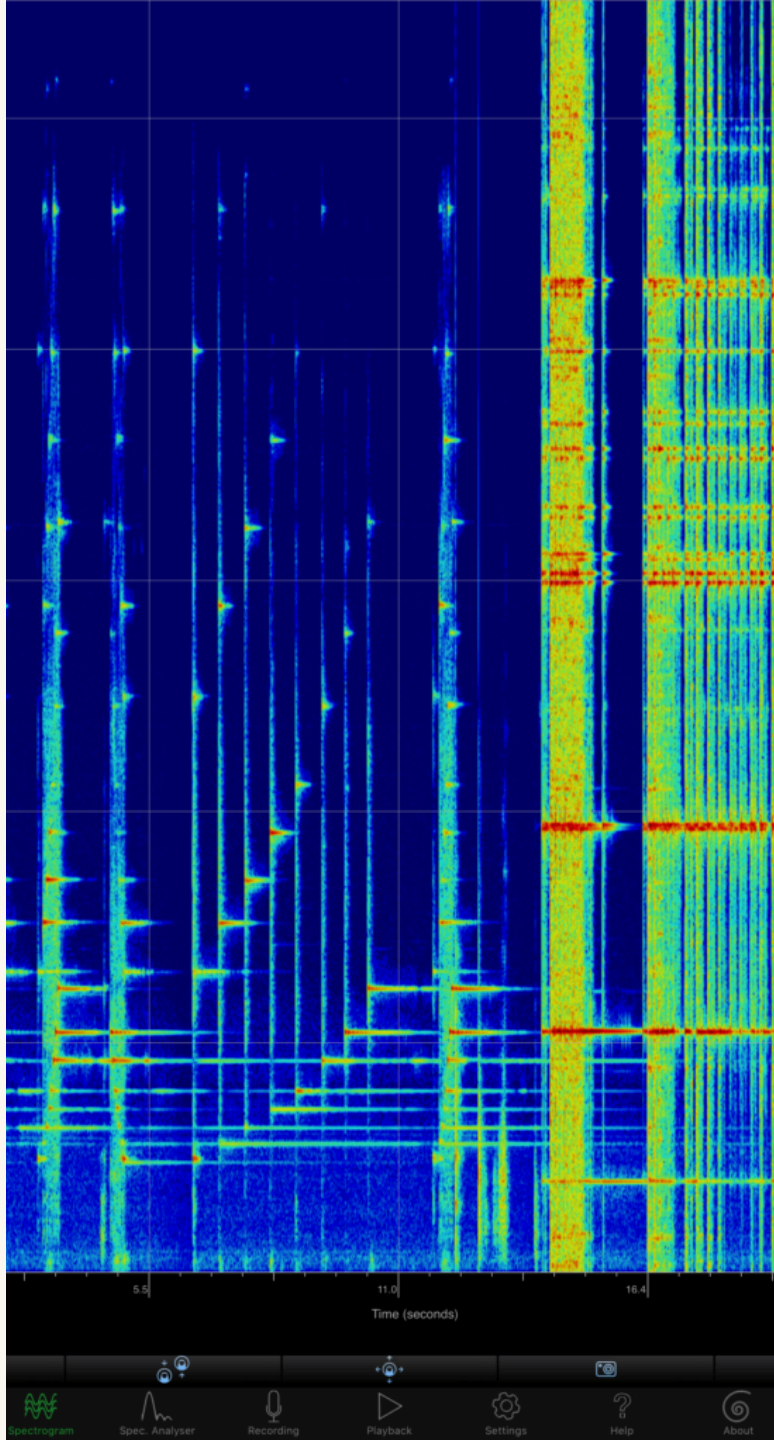
- Ensure that the source used **disposable equipment** not tied to them.
- Ensure that the documents were **not directed** to the source.
- Sanitize documents before publication:
  - Dangerzone (GUI)
  - MAT2 (CLI-only)

OPSEC works!

KRIK protected their source by not providing the prosecutors office with the original recording of an incriminating discussion.

> *In its latest letter to KRIK, the prosecutor's office claims the recording is needed for forensic examination and insists it is not asking the newsroom to reveal its source, only to* ***provide the recording itself — either the original, its "closest copy," or the device on which it was recorded.*** *The letter again threatens journalists with a* ***fine if they fail to comply****.*

Source: OCCRP — Serbian Prosecutors Threaten KRIK with Fine if it Fails to Submit Recording of a Conversation

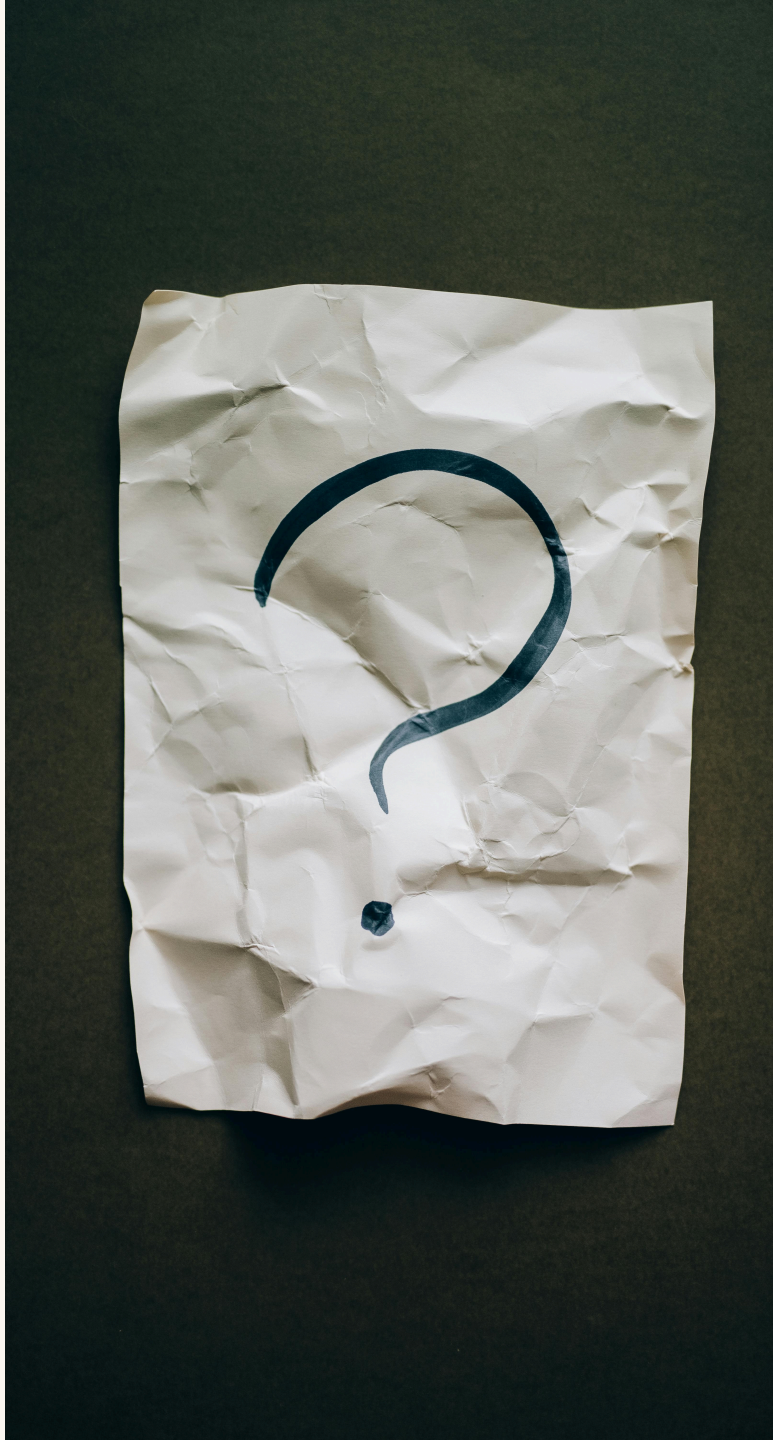


OPSEC works!

Radio New Zealand protected their source by not disclosing the document format that the source provided to them.

> *[...] the investigator interviewed more than **40 people** including those who accessed the Budget report **"via SharePoint"**, received a copy of the report as an **email attachment**, or **had printed it**. [...] It was unclear which version the reporter had seen.*
>
> *The Investigator asked to speak to the RNZ reporter [...] to discuss matters such as **the file format and version of the Budget Report disclosed to him**. The reporter and Radio New Zealand via its legal representation declined to do so.*

Source: Radio New Zealand — Ministry of Education's $20,000 inquiry fails to find Budget leak to RNZ



Thank you

Questions? OPSEC war stories?