Cryptohagen 10 Years Anniversary

Alexander Hansen Færøy <ahf@0x90.dk>

About

- Free software developer since my teenage years. Linux primarily because my laptop kept rebooting under Windows.
- Gentoo, MIPS Linux, Qt, WebKit, OpenWRT, Erlang, Irssi, a lot of the ircd’s, …
- These days leading the Anonymity team at The Tor Project.
- BornHack co-founder.
- Early Cryptohagen attendee. Met my partner in this space. Pretty bad at showing up :-(

The Early Post-Snowden Period

- Cryptoparties! Teaching everybody about all the tech. Some people wanted more focus on usability.
- Messaging: OTR, OMEMO, MP-OTR, PGP for everything, …, the quest for the holy grail of messaging via Jabber, IRC, Facebook Chat. Remember SMP?
- Deniability was still a big sales argument.
- The free software community was strong here, but as always, we also had very strong opinions and many things mattered very little in the end.
- The TLS ecosystem and the arrival of Let’s Encrypt.

The Early Post-Snowden Period

- RedPhone / TextSecure -> Signal.
  - Strong focus on usability, deployment, and end-users.
  - “Protocol agility” and decentralization left out in the design.

- Watch Moxie’s talk from 36c3: “The ecosystem is moving.” Alas, the video was taken down, but it’s possible to find on The Internet.

The Intercept_

U.S. OFFICIALS CALLED SIGNAL A TOOL FOR TERRORISTS AND CRIMINALS. NOW THEY'RE USING IT.

Despite years of official criticism of encrypted messaging, CIA Director John Ratcliffe revealed that Signal comes installed on agency computers.

Matt Sledge

March 25 2025, 6:42 p.m.

Share

The Guardian

Signal group chat leak

Pentagon warned staffers against using Signal before White House chat leak

Bulletin sent on 18 March said Russian hackers could access messages as Trump officials now downplay blunder

José Olivares

Tue 25 Mar 2025 20.19 CET

Share

Top national security officials inadvertently added a journalist to a Signal group chat discussing plans for military strikes in Yemen. Photograph: Thomas Trutschel/Photothek via Getty Images

Eur
The Guardian

News Opinion Sport Culture Lifestyle

World Europe US Americas Asia Australia Middle East Africa Inequality Global development

Signal group chat leak

Judge orders participants in Signal chat group blunder to preserve all messages

Restraining order was issued to ensure that records of Yemen attack group conversation are retained

Hugo Lowell *in Washington*

Fri 28 Mar 2025 00.53 CET

Share

Most viewed

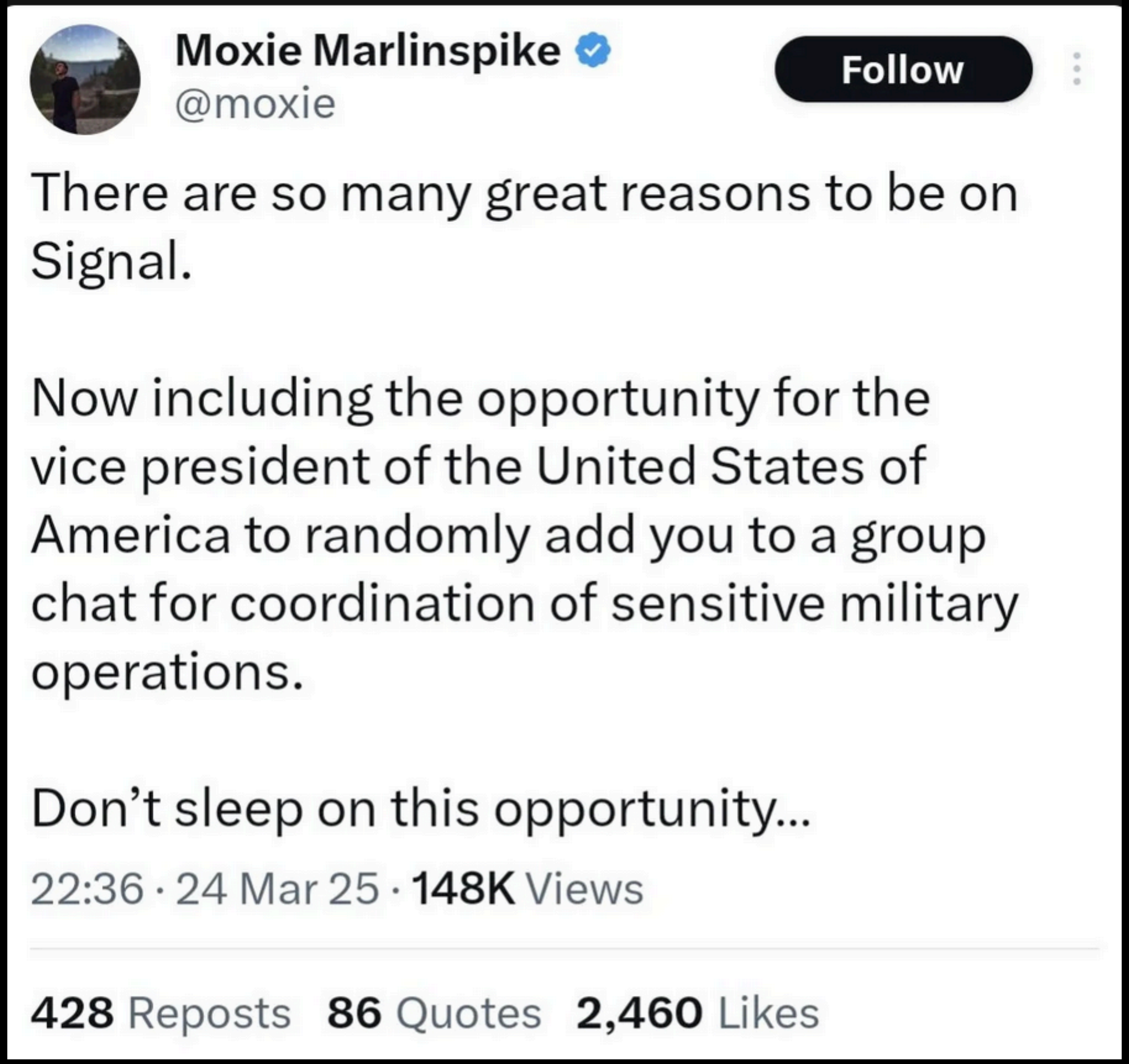
Scramble to free survivors as death toll passes 1,600 after Myanmar earthquake

A tip for JD Vance: Greenland doesn't care about your frail human ego
Sarah Ditum

Protests hit Tesla dealerships across the world in challenge to Elon Musk

Alarm as Florida Republicans move to fill deported workers' jobs with children: 'It's insane, right?'

Le boycott: French customers shun McDonald's, Coca Cola and Tesla to protest against Trump



Moxie Marlinspike
@moxie

There are so many great reasons to be on Signal.

Now including the opportunity for the vice president of the United States of America to randomly add you to a group chat for coordination of sensitive military operations.

Don’t sleep on this opportunity...

22:36 · 24 Mar 25 · 148K Views

428 Reposts 86 Quotes 2,460 Likes

System Security

- State vs. Stateless and .
- Reproducible Builds.
- Boot security and “State considered harmful”.
- QubesOS and Tails.
- Kernel and user-space hardening, stricter languages => improved “correctness”.
- Leaving memory unsafety behind.

Epic Security Bugs Needs an Epic Name!

- Heartbleed, 2014.
- Shellshock, 2014.
- Ghost, glibc, 2015.
- Rowhammer, “2014”.

The Industrial Anonymity Complex

- MASQUE and Big Tech’s hunt for an industrial anonymity system (with zero fucks given for Side Channel attacks).
- Apple’s CEO “Porn mode” for iPhone (iCloud+ subscription).
- CDN providers and Google.

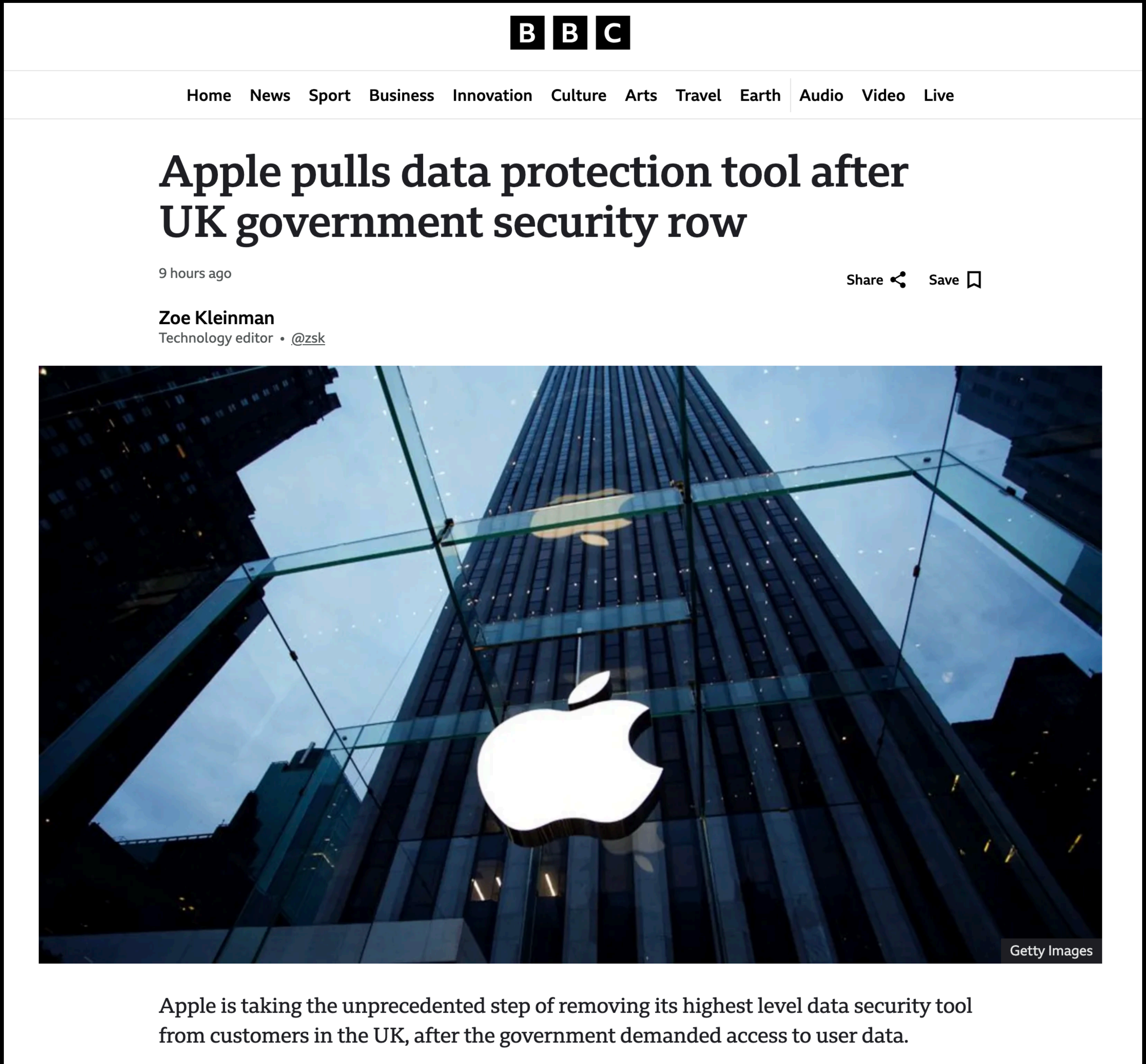
Are we adequately encrypted?

- The fear of the potential arrival of the Quantum computer.
- Partially getting energized by the same hype-people who really think AGI (AI) is just around the corner.
- We have some of the tools to solve this, we think, but deployment is not as easy for everybody. Widespread adoption (TLS) will likely take at least a full cycle of FOSS OS upgrades.

Power Centralization of the Web

- Big players largely controls the web these days.
- IETF is following along.
- EU is being somewhat helpful with the browser monopoly, but Apple is still a difficult actor in this game.

GDPR



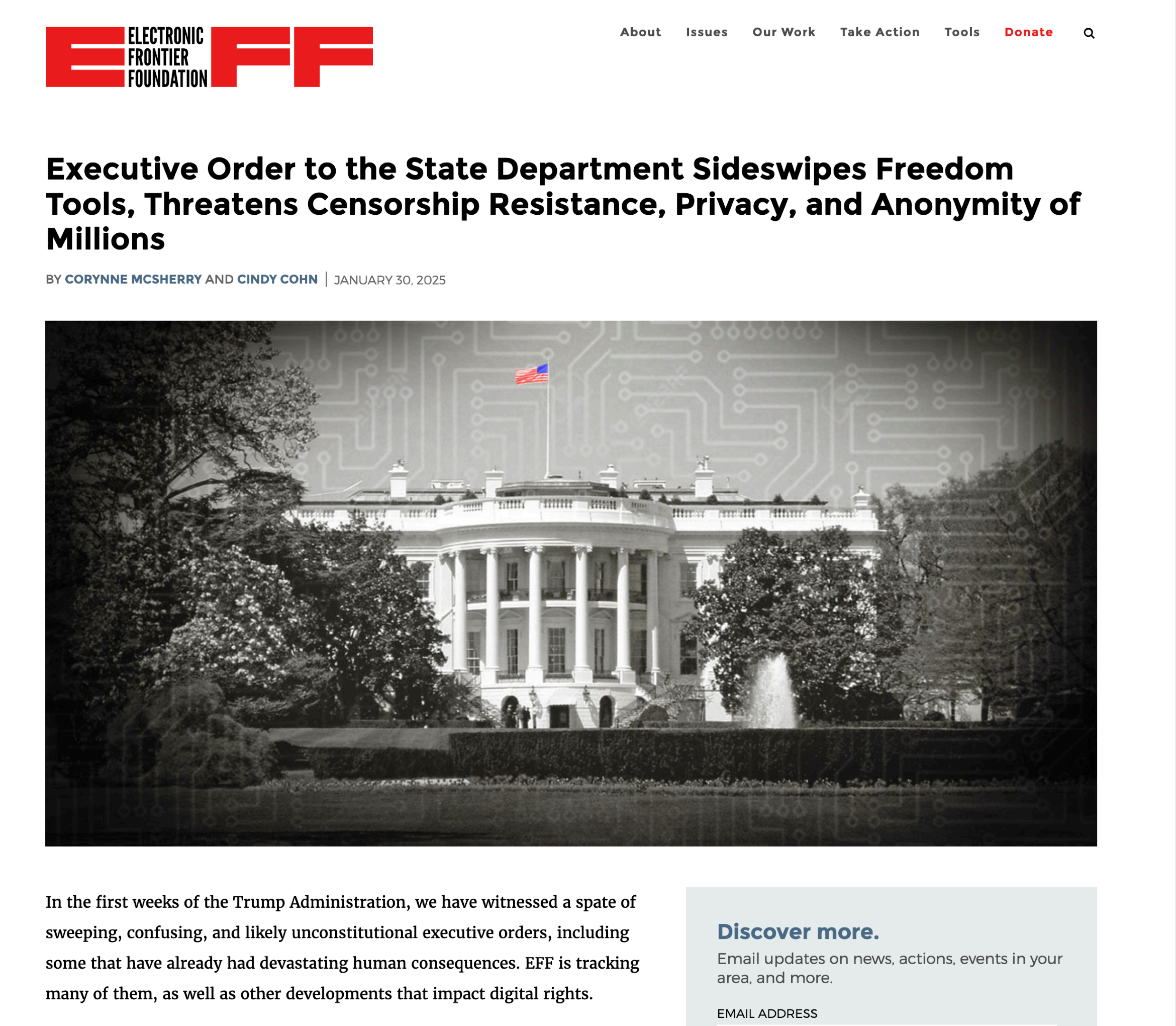
Apple pulls data protection tool after UK government security row

9 hours ago

Zoe Kleinman
Technology editor • @zsk

Getty Images

Apple is taking the unprecedented step of removing its highest level data security tool from customers in the UK, after the government demanded access to user data.



Executive Order to the State Department Sideswipes Freedom Tools, Threatens Censorship Resistance, Privacy, and Anonymity of Millions

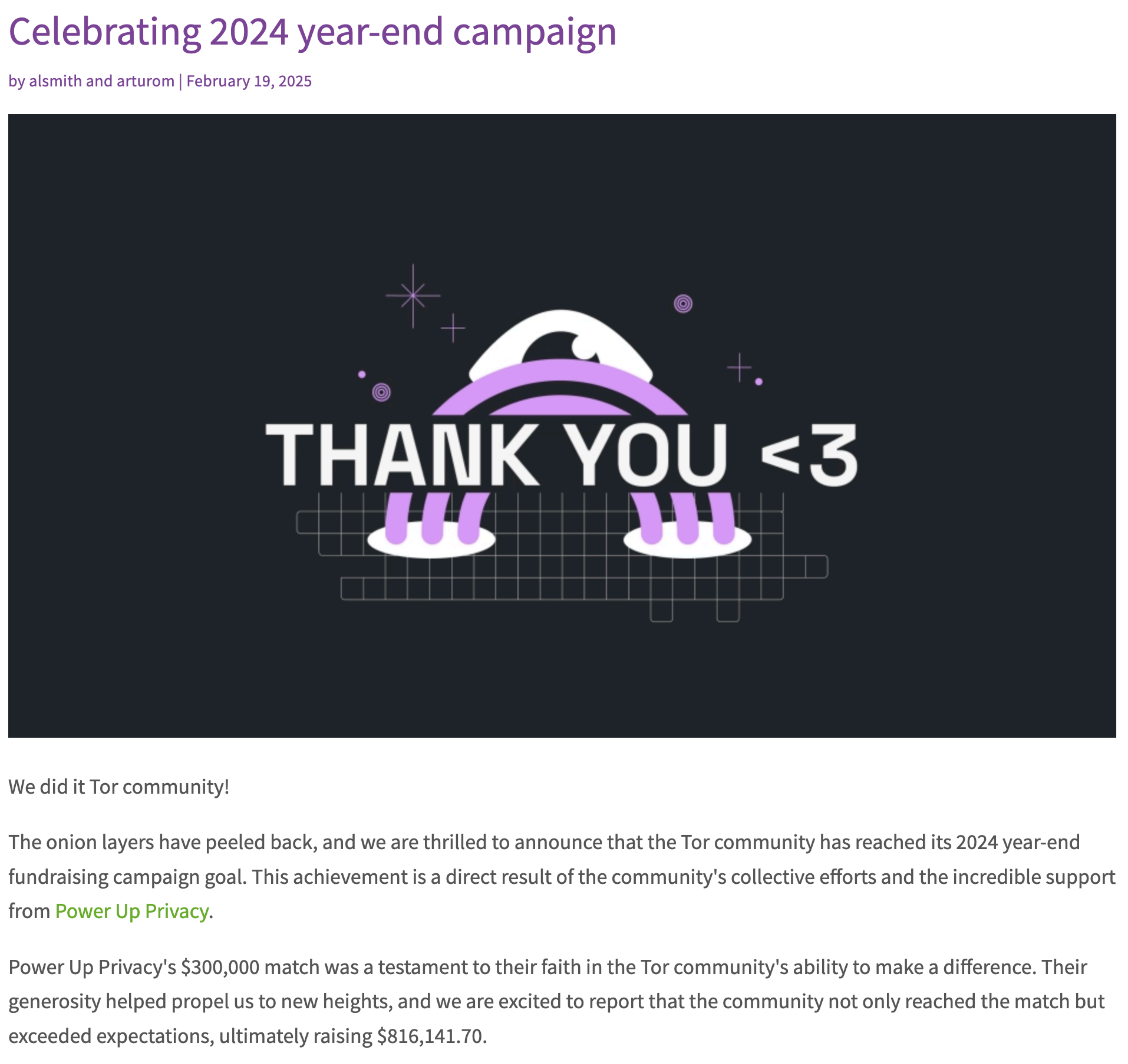
BY CORYNNE MCSHERRY AND CINDY COHN | JANUARY 30, 2025

In the first weeks of the Trump Administration, we have witnessed a spate of sweeping, confusing, and likely unconstitutional executive orders, including some that have already had devastating human consequences. EFF is tracking many of them, as well as other developments that impact digital rights.

Discover more.

Email updates on news, actions, events in your area, and more.

EMAIL ADDRESS



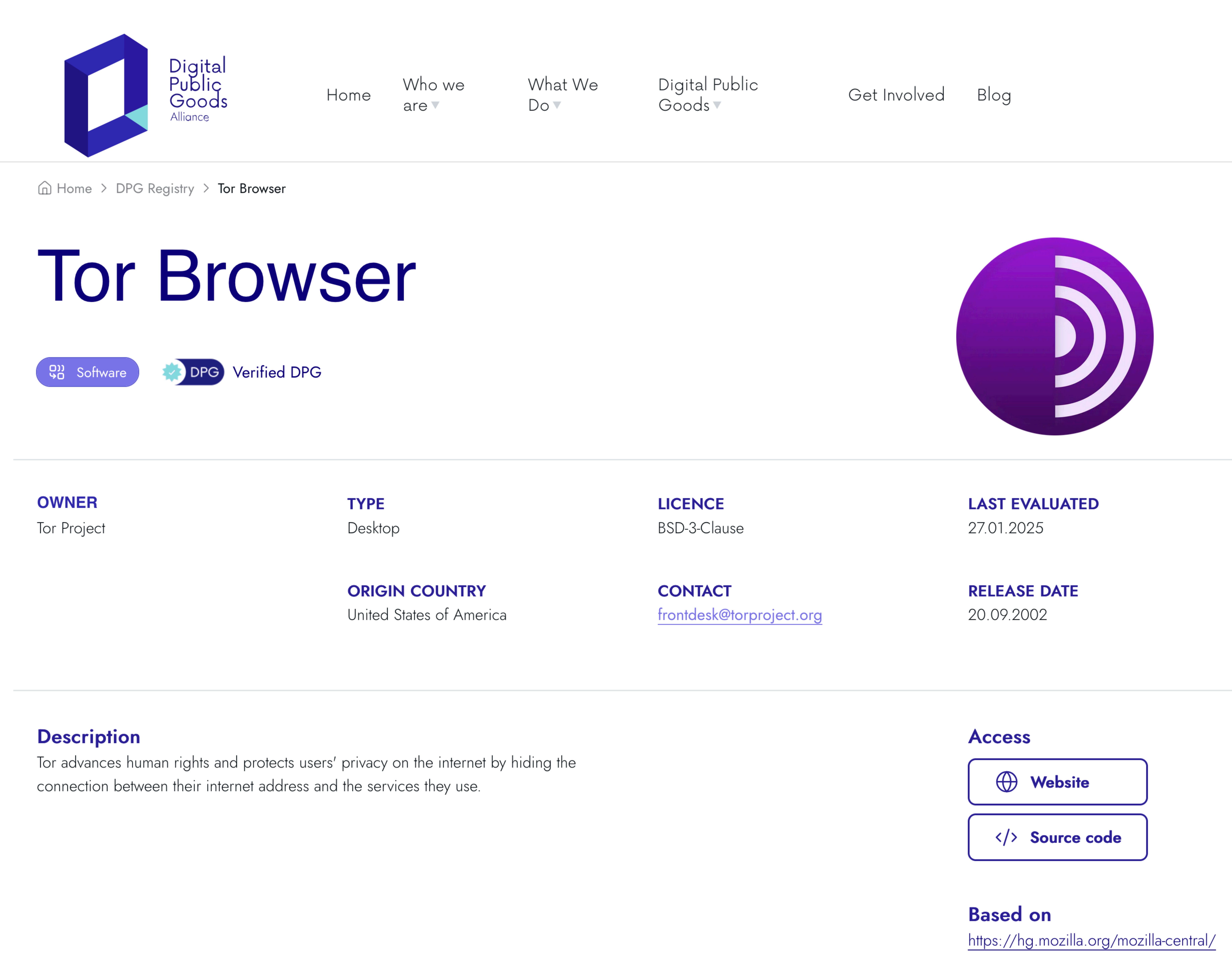
Celebrating 2024 year-end campaign

by alsmith and arturom | February 19, 2025

We did it Tor community!

The onion layers have peeled back, and we are thrilled to announce that the Tor community has reached its 2024 year-end fundraising campaign goal. This achievement is a direct result of the community's collective efforts and the incredible support from Power Up Privacy.

Power Up Privacy's $300,000 match was a testament to their faith in the Tor community's ability to make a difference. Their generosity helped propel us to new heights, and we are excited to report that the community not only reached the match but exceeded expectations, ultimately raising $816,141.70.


Digital Public Goods Alliance
Home
Who we are
What We Do
Digital Public Goods
Get Involved
Blog
Home > DPG Registry > Tor Browser

Tor Browser

OWNER	TYPE	LICENCE	LAST EVALUATED
Tor Project	Desktop	BSD-3-Clause	27.01.2025
	ORIGIN COUNTRY	CONTACT	RELEASE DATE
	United States of America	frontdesk@torproject.org	20.09.2002

Description

Tor advances human rights and protects users' privacy on the internet by hiding the connection between their internet address and the services they use.

Access

Based on

https://hg.mozilla.org/mozilla-central/

Get Snowflake

Free your connection

Use Snowflake to give censorship the slip in places where Tor is blocked.

BLOCKED USER

Start using Snowflake Now

Snowflake comes embedded in Tor-powered apps like Tor Browser and Orbot . If either of these apps can't connect to the Tor network, you can use Snowflake to unblock Tor.

Read the FAQs

Tor Browser

Get it from:

torproject.org/download

Available for
Desktop & Android

Snowflake
Ready to Use

Made by
Tor Project

Orbot

Get it from:

orbot.app

Available for
Android & iOS

Snowflake
Ready to Use

Made by
Guardian Project

Tor
Tails

Application Isolation

- You want to run an application over Tor. You have two options:
  - Use Tor’s SOCKS or HTTP proxy feature.
  - Use a tool, such a torsocks that uses an LD_PRELOAD hack to hook into the C standard library’s network API.

SOCKS and HTTP Proxy

- Many applications today comes with SOCKS support, but it’s a dying piece of technology in the modern web world.
- Applications must actually get everything right, otherwise you have a leak.
  - Few people test for actual leaks.
- Must be implemented for every application that you want to use.

Torsocks

- Used for applications, that does not support SOCKS/HTTP proxies, but that you wish to route via Tor.
- Hooks into the C library, particularly connect(2) and the DNS layer.
- Is only able to isolate calls coming from the C library.
- “Raw system calls” not supported.
- Support is difficult on multiple platforms, including macOS these days.
- A massive hack.

Linux Namespaces

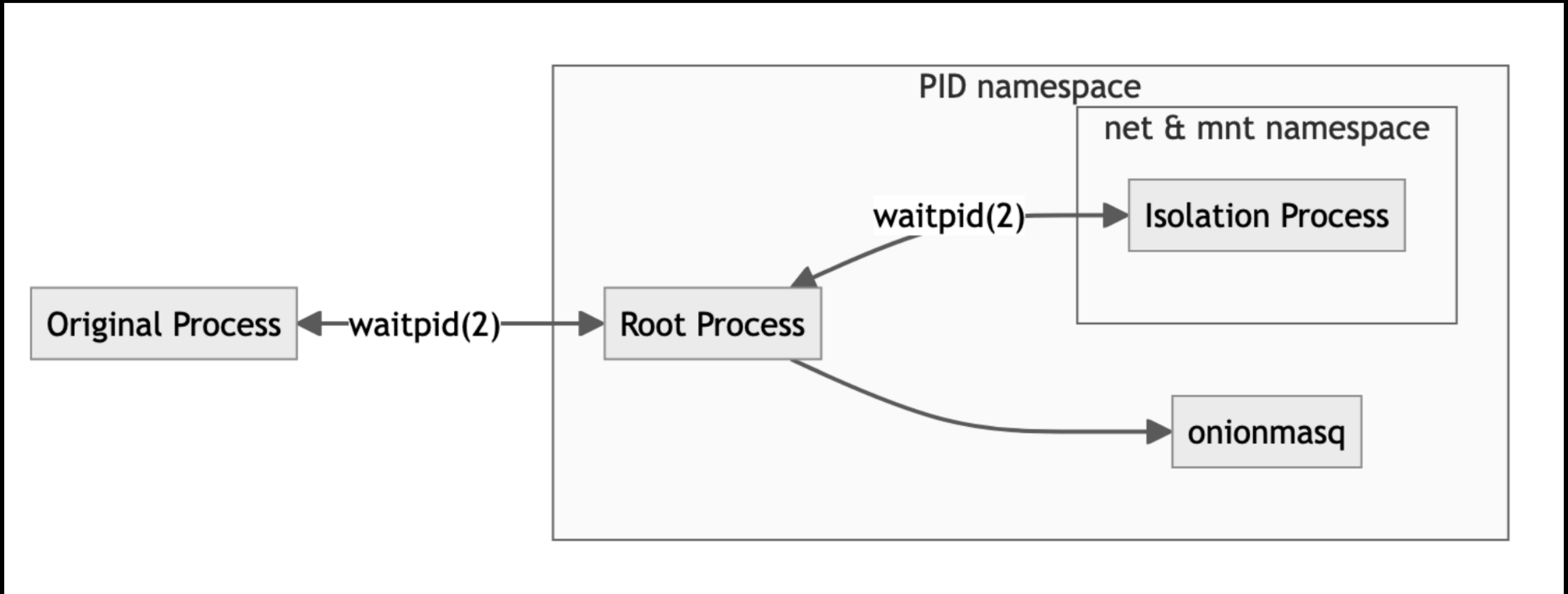
- Today we can isolate a lot of different kernel resources per process.
- Namespaces supports multiple different features:
  - PID namespace.
  - Mount namespace.
  - Network namespace.
  - Time namespace.
  - …

Onionmasq

- Uses Tor’s Arti implementation to create a TUN-interface.
- Handles packets instead of TCP flows:
  - Multiplexes the 5-tuple network flows via Tor streams.
  - Handles isolation tokens.
  - Fakes DNS by providing a DNS resolver on the TUN-interface (for .onion support and more).

Oniux

- Use Linux Namespaces with Onionmasq:
  - Runs in a PID namespace.
  - Launches the Onionmasq process.
  - Launches the target child process in a mount and network namespace.
  - Ensures the Onionmasq TUN interface is configured into the target child’s network namespace.
  - Uses capabilities, so can be installed as root, and won’t need root permissions afterwards.


PID namespace
net & mnt namespace
waitpid(2)
Isolation Process
Original Process
waitpid(2)
Root Process
onionmasq

Pros and Cons

- Anti-leak guaranteed by the operationg system.
- Applications does not need to be aware of the underlying Tor layer.
- Much less hacky.

- Highly Linux centric.
- No central daemon right now.
- Early stage prototype.
- Capabilities are good, but difficult for ephemeral configurations.

- Arti adoption in Tails and Tor Browser.
- Research into sandboxing options for apps with system-wide Arti.

Left out for another speaker

- New(er), federated, social media platforms.
- Leaving “Big Tech” behind.
- Denmark specific legal situation(s) and politics.
  - “FE Sagen” with Lars Findsen.
- Copyright re-assignment in the corporate FOSS world.

The next ten years?

- Return to focus on Free Software?
- Hopefully, cryptography will continue to get “more boring” => “invisible”.
- We will still need spaces to socialize, teach, counter FUD, counter “I heard from a friend that X, Y, and Z is (bad|pwned|controlled by an evil actor)”.
- Will cryptography become a tool for the privileged?

Questions?

ahf@0x90.dk

@ahf@mastodon.social