PROTOCOL SYMPOSIUM 2026, NEW NATURE

Entrenching Privacy Through Speech

Privacy technology is infrastructure for expressive freedom.

Jesse Katz, Speech Without Borders
with Eric Alston, University of Wyoming College of Law

Who I am, and what I'm not

- Speech Without Borders (speech.ngo) is a 501(c)(3) nonprofit initiative supporting the development and distribution of technologies and policies that advance and defend expressive freedom.
- I've built infrastructure for social protocols that help decentralize social media, and I spent a decade running a marketing studio, which shapes how I approach privacy advocacy.
- I'm not a lawyer or an academic, and I'm not speaking as an authority. I'm narrating a process of learning.
- My co-author and SWB advisor, Eric Alston, spoke earlier today. SWB, and this paper in part, sit at the intersection of much of his work, which you can find at incompleterules.com

It started as an intuition

- The goal was a short memo for the Ethereum Foundation, backed by just enough research to support persuasive arguments.
- A big part of marketing is tailoring messaging to target audiences, and privacy has been a hard sell. The spark was Danny Ryan reframing decentralization as the elimination of counterparty risk, a reframe that worked because it was accurate.
- Privacy is litigated as a prerequisite for speech and association in the United States, and that relationship can be useful in privacy advocacy outside the courtroom as well.
- This topic couldn't be covered at a surface level, so I kept digging, and it turned into something much more interesting.

Where technical, social, and legal protocols intersect

- This talk follows the structure of our paper. What you'll hear is Part I, a conceptual overview. Part II is built to load into an LLM as a substrate for privacy messaging, like an index with pointers to sources. The paper is in the symposium folder.
- Our analysis focuses on Ethereum, but the argument is not specific to Ethereum. It applies wherever privacy technologies support expressive activity.
- The argument moves in three steps, from the gap in US privacy law, to what decentralized technology can make durable, to the First Amendment protections that can give it standing.
- It is appropriate for privacy-focused projects to lead with privacy, and expression is only an additional tool for how the ecosystem talks about, funds, develops, and organizes around it.

Anything sufficiently decentralized comes down to social coordination

- Privacy is contentious, so how we talk about it is part of the coordination.
- The Ethereum Foundation's 2026 Mandate names privacy one of four non-negotiable core properties, alongside censorship resistance, open source, and security, which together it calls CROPS.
- Nation states will hear "non-negotiable" the way they hear an aspiring network state, as a claim of exit. The better message is membership in an order that already protects you.
- Messaging around CROPS values should communicate that the technology supports and is compatible with existing rights and laws. The point is practical and tactical, and it misrepresents nothing.

The only G20 nation without a comprehensive federal privacy law

- For decades, data shared with any third party lost its protection in the United States, and the protections still stop short of information disclosed openly. A public blockchain is open by design.
- This gap persists for a structural reason. The government benefits from access to this information, and private companies profit from collecting and selling it, including to the agencies that would otherwise need a warrant to obtain it.
- Alston and Cossar call this perverse alignment the institutional privacy dilemma, and it explains why federal privacy legislation keeps failing.

Durable in a way law alone cannot make it

- Our analysis focuses on areas where there are no trusted operators. People who build and run decentralized systems cannot arbitrarily change their rules or hand over user data they do not have.
- Decentralized, credibly neutral technologies can make privacy durable, encoding commitments that no person, company, or government can revoke. Legal protection, in turn, gives those commitments the standing of a right courts already enforce.
- In Josh Stark's terms, blockchain hardness holds the commitment and institutional hardness defends it. That is the sense of entrenching in our title, and it connects to Eric's talk on governance axioms.

What Tornado Cash is evidence for

- Regulation by enforcement deters people from building and using legitimate privacy tools for lawful purposes.
- After Tornado Cash, a decentralized privacy tool with no trusted operators, was sanctioned and its developers prosecuted, users and builders were observably less inclined to risk touching privacy tools.
- The pressure fell on lawful use first, and it weakened the tool for unlawful users only by driving lawful ones out.
- The Ethereum Foundation has committed to privacy at the protocol level. Ethereum is public by default, so privacy has to be built in.

Privacy has long been protected under the First Amendment's freedoms of speech and association

- Without that privacy, exposure deters participation. Courts have protected membership lists and donor records for exactly that reason.
- The First Amendment protects expression far more robustly than any US law protects privacy, and that gap is why relating privacy to expression might be useful, legally and rhetorically.
- Activities like funding causes and participating in governance are now happening on Ethereum, and they should be similarly protected, at the very least.

Ethereum should be recognized and protected for the expression it enables, like the internet

- Open communication systems that let people freely speak, publish, and organize have earned constitutional protection of their own as general-purpose infrastructure. That protection did not depend on the proportion of expressive use.
- When the Supreme Court took up the internet, it looked at what the medium made possible, where any person can become a town crier, and it later declined to judge a young medium by the uses its critics emphasize.
- There are strong arguments for extending similar protection to Ethereum, and courts are still working out how existing rights translate to these new technologies.

A single transaction can be a payment, a vote, and a signal of membership and identity, all at once

- In funding rounds where contributions double as votes, one transfer moves the money, helps decide which projects are funded, and permanently marks what the sender supports.
- Disentangling protected expressive activity from ordinary traffic would require reviewing every transaction for its purpose, the very surveillance the First Amendment guards against.
- Public-by-default transparency was the price of trustless verification with the cryptography available at the time. The exposure was a consequence, and privacy is the remedy.
- This is the most ambitious argument and not yet tested. The proposed standard preserves legitimate enforcement while barring the wholesale review that chills expression.

The privacy of thought

- The structural relationship between speech and privacy should apply wherever privacy technologies support expressive activity, and AI and neurotechnology are where the analysis extends next.
- The AI tools people reason and draft with capture thinking in progress, and the dependence on privacy only deepens as augmented intelligence moves closer to the mind.
- Brain-computer interfaces may be where expression doctrine reaches its limit, and that is where privacy needs protection on its own terms.
- Protecting privacy through expressive rights can risk making privacy look merely instrumental, and the work of building privacy protections that stand on their own continues.

Does privacy already stand on its own?

- I'd like to explore whether, on a better reading of the law we already have, there is an independent right to protect our own privacy by our own means, one the state may not forbid.
- A person may provide for their own protection against a real threat, and the state may not take away the means of doing so. Nobody has to wait for an intruder at the door to be allowed a lock.
- The government owes no constitutional duty to protect us from other people, so the right to protect ourselves is strongest exactly where the state's duty runs out.
- This is exploratory, and I want to see where it leads.

This research quickly outran me

- It relies on contributions from others, who ought to be credited, and it should leave room for discourse wherever we disagree.
- The intent is to share the research alongside the writing, as a knowledge commons and an open dataset others can build on. We're planning experiments in this with the California Institute for Machine Consciousness (CIMC).
- Sreeram Kannan's work at Eigen Labs, where open networks of people and AI agents build on each other's verified results, shows how protocols can organize research, here and across the topics at this conference.

Privacy technology is infrastructure for expressive freedom.

Ethereum is one part of it. Its protocol layer merits protection under the First Amendment, because the expression it enables cannot function without privacy, and the same relationship holds wherever privacy technologies support expressive activity.

The paper is in the symposium folder. Read Part I in a few minutes, or load Part II into your model.

Questions, disagreement, and collaborators welcome.

speech.ngo