Naming the Harm

A privacy threat vocabulary for cypherpunks

Daniel Calderon, Mate Soos

June 14, 2026

LINDDUN

The state of privacy in crypto, 2026

LINDDUN

- **Roman Storm** (Tornado Cash co-founder/developer) convicted Aug 2025 for unlicensed money transmission. Jury hung on the money-laundering and IEEPA-sanctions counts; *Writing privacy code is being prosecuted as a crime.*
- **Tornado Cash**: OFAC-sanctioned Aug 2022; in 2024 held OFAC exceeded its authority over smart contracts; Treasury delisted 2025 (Semenov still SDN under the DPRK sanctions program). *The reversals don't undo the chill on developers*
- **Chain analysis as an industry**: Chainalysis, Elliptic, TRM Labs — provide clustering and attribution services to exchanges, regulators, and law enforcement
- **KYC leaks**: Ledger & exchange breaches — real identities tied to on-chain history
- **Mempool surveillance**: MEV searchers and front-runners watch every pending transaction

We need a precise way to talk about which privacy property is violated and how.

Privacy is not Security

- **Security**: who can *access or alter* the data?
- **Privacy**: even with perfect access control, what does the *authorized* party learn, infer, or share about a person?
- **Ethics**: should we collect or process this data *at all*?

Why this matters for cypherpunks.

- A KYC database can be *perfectly secure* and a privacy disaster — central aggregation, secondary use, leak risk
- A signed on-chain transaction is a *security feature* (authenticity, integrity) and a privacy disaster (public, eternal attribution)

Cypherpunks already think hard about security; LINDDUN is the matching vocabulary for privacy

Why this talk?

- "Privacy is necessary for an open society in the electronic age." — Eric Hughes, *A Cypherpunk's Manifesto*, 1993
- 33 years later, we still debate surveillance without a shared vocabulary for the privacy properties we want
- **LINDDUN** is a precise taxonomy of privacy harms we face — built in academia, cited by regulators, but rarely used in our circles

What is LINDDUN?

- A privacy threat modeling framework
- Developed at **KU Leuven** by Deng et al. (*Requirements Engineering* 16:3–32, 2011)
- Explicitly analogous to the STRIDE security framework
- NIST's Privacy Framework Resource Repository lists LINDDUN as a compatible threat-modeling resource; GDPR Art. 25 ("Data protection by design and by default") is the legal hook it operationalizes.

Goals.

- Systematically *elicit* privacy threats in a system, so none are missed by intuition
- Map each threat to concrete *mitigations* — making privacy tradeoffs explicit

Privacy harms across the data lifecycle

Collection

- Detecting

"Did the user know? Did they consent?"

Processing

- Linking
- Identifying

"What can we infer?"

Sharing / Output

- Data Disclosure

"Who else sees it?"

Different harms bite at different stages — the same protocol can be clean at one stage and disastrous at another.

Adapted from Solove's privacy harms taxonomy (Collection / Processing / Dissemination / Invasion).

The 7 privacy harms

LINDDUN

	**L**inking	Associating data items or user actions to learn about an individual or group
	**I**dentifying	Learning the identity of an individual
	**N**on-repudiation	Attributing a claim to an individual; loss of plausible deniability
	**D**etecting	Deducing involvement of an individual through observation
	**D**ata Disclosure	Excessively collecting, storing, processing or sharing personal data
	**U**nawareness & Unintervenability	Insufficiently informing, involving, or empowering the data subject
	**N**on-compliance	Deviating from privacy best practices, standards, and legislation

Definition. Associating data or actions to learn about an individual — without necessarily knowing who they are.

Real-world. Target identified pregnant customers from shopping patterns and mailed baby coupons before relatives knew. *No name, no PII — just linked records.*

Crypto. Chain-analysis clustering: co-spending heuristics, address reuse

Mitigation. **stealth addresses** (ERC-5564) put each payment on a fresh address.

Definition. Learning the identity of an individual from nominally pseudonymous data.

Real-world. **AOL search log leak (2006)**: 658k "anonymized" search histories released; NYT identified user 4417749 as Thelma Arnold within days. *Pseudonyms are not anonymity.*

Crypto. One KYC'd exchange deposit ties a real identity to an address

Mitigations. **zk-SNARKs** (Zcash, Aztec) hide sender, recipient, amount

Definition. Attributing a claim to an individual — eliminating plausible deniability.

Real-world. **Nebraska abortion case (2022)**: Meta surrendered Facebook Messenger DMs between a mother and her 17-year-old daughter under warrant; both pleaded guilty. *Messages they thought were ephemeral became durable courtroom evidence.*

Crypto. Every signed transaction is permanent, public evidence

Mitigation. **shielded transactions** (Zcash) leave no public attribution

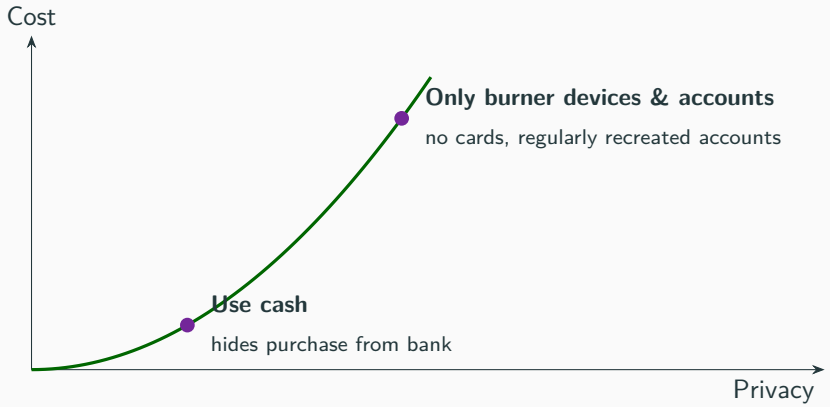
Definition. Deducing the involvement of an individual through observation — even without seeing content.

Real-world. **Strava heatmap (2018)**: aggregated "anonymous" fitness data exposed perimeters and patrol routes of secret US military bases in Syria, Niger, Afghanistan. *Metadata alone was the breach.*

Crypto. *The fact that* a transaction occurred is sensitive

Mitigations. **Mixnets** (Nym), **onion routing** (Tor) anonymize the network layer

Concrete tradeoffs — privacy is not free



LINDDUN doesn't tell you which tradeoff to make — it tells you what you are trading.

What LINDDUN does *not* model

- **Adversary-agnostic.** A state intelligence agency, a chain analysis firm, and a curious neighbor are the same "adversary" to LINDDUN.
- **No power asymmetry.** The harm to a journalist surveilled by their government is not the harm of an ad-tracking pixel — LINDDUN treats both as "Identifying."
- **No coercion.** A consent dialog satisfies *Unawareness* — but consent under threat of being unbanked, deplatformed, or denied service is not consent.
- **No political economy.** Who profits from the data? Who is forced to produce it? LINDDUN doesn't ask.

LINDDUN is a precise vocabulary, not a political theory. Bring your own politics.

Takeaways

- LINDDUN gives cypherpunks a **precise vocabulary** for privacy harms — the same one regulators use. Speak it fluently to argue back.
- Each of the 7 harms maps to **concrete crypto attack patterns** and to a **matching PET**.
- Privacy is a **spectrum of tradeoffs**, not a binary; LINDDUN structures the conversation but doesn't make the choice for you.

What you can do to help.

- Pick a wallet, dApp, or protocol you depend on. Run LINDDUN on it.
- Publish the threat model. Make privacy a deliverable, not a marketing claim.
- Engage in the policy conversation about privacy-preserving code.

Questions?

- Deng, Wuyts, Scandariato, Preneel, Joosen. *A privacy threat analysis framework supporting the elicitation and fulfillment of privacy requirements*, 2010. https://link.springer.com/article/10.1007/s00766-010-0115-7
- LINDDUN homepage: https://linddun.org/
- LINDDUN threat types: https://linddun.org/threat-types/
- NIST Privacy Framework Resource Repository — LINDDUN entry: https://www.nist.gov/privacy-framework/linddun-privacy-threat-modeling-framework
- NIST Privacy Framework v1.0: https://www.nist.gov/system/files/documents/2021/05/05/NIST-Privacy-Framework-V1.0-Core-PDF.pdf
- EU GDPR: https://gdpr-info.eu/

- GDPR Art. 4 (definitions): https://gdpr-info.eu/art-4-gdpr/
- Privacy-Enhancing Technologies (Wikipedia): https://en.wikipedia.org/wiki/Privacy-enhancing_technologies
- Hansen, "Privacy Terminology" (IETF draft, 2010): https://datatracker.ietf.org/doc/id/draft-hansen-privacy-terminology-00.html
- LINDDUN 2015 threat-modeling guide: https://www.cs.kuleuven.be/publicaties/rapporten/cw/CW685.pdf
- Solove, *A Taxonomy of Privacy*, U. Pa. L. Rev. 154:477, 2006. https://scholarship.law.upenn.edu/penn_law_review/vol154/iss3/1/
- Duhigg, *How Companies Learn Your Secrets* (Target pregnancy prediction), New York Times, 2012. https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

- Barbaro & Zeller, *A Face Is Exposed for AOL Searcher No. 4417749*, New York Times, 2006. https://www.nytimes.com/2006/08/09/technology/09aol.html
- Hsu, *Facebook turned over teen's DMs to Nebraska police in abortion case*, Washington Post, 2022. https://www.washingtonpost.com/technology/2022/08/12/nebraska-abortion-case-facebook/
- Hern, *Fitness tracking app Strava gives away location of secret US army bases*, The Guardian, 2018. https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

- Cadwalladr & Graham-Harrison, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica*, The Guardian, 2018.
  https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election
- Irish DPC, *Decision in TikTok GDPR investigation*, 2023.
  https://www.dataprotection.ie/en/news-media/press-releases/dpc-announces-345-million-euro-fine-tiktok
- Irish DPC, *Decision on Meta EU–US data transfers*, 2023.
  https://www.dataprotection.ie/en/news-media/press-releases/Data-Protection-Commission-announces-conclusion-of-inquiry-into-Meta-Ireland