Policy threats to encryption

Mallory Knodel – PEARG IETF 124

Global scan of policy challenges to e2ee

- Resource: https://www.gp-digital.org/world-map-of-encryption
- Europe
  - ChatControl
  - Sweden
  - France
- Asia
  - India
- North America
  - Canada

Policy-motivated technical challenges

- Client-side scanning
  - IAB statement
  - IAB Open @ IETF 122
- Link tracking
- Traceability

Client-side scanning

CSS shifts surveillance to the user’s own device, scanning content before encryption.

- Scans occur prior to message encryption — every photo, text, or file is analyzed locally.
- Uses hash-matching or AI classifiers to flag “harmful” or “illegal” content.
- Undermines endness and the end-to-end security model.
- Creates systemic risks.
- Exploitable scanning pipelines.
- Expansion to non-targeted content (mission creep).
- Chilling effect on free expression and association.
- Consentless, pre-emptive, and suspicionless…
- No such thing as ‘client-side scanning of illegal content’; client-side scanning means scanning of *all* content”.

Link tracking

Link and click tracking for the purposes of attribution or pay-per-view enforce scanning and leak behavioral data that can be repurposed for surveillance and policy enforcement.

- Requires message content.
- Tracking parameters (e.g., utm_source, unique IDs) embedded in URLs identify users and recipients.
- Enables re-identification and correlation across services — “who clicked what, when, from where.”
- Once normalized, link tracking becomes a traceability layer that defeats privacy and anonymity.

Traceability

Traceability laws compel platforms to record and disclose who originated every message, destroying deniability and unlinkability.

- Enhanced metadata.
- Requires service providers to hash and store every message with origin data, maintaining a searchable trail.
- Breaks a key property of secure messaging: sender anonymity and plausible deniability.
- Inevitably turns E2EE systems into logging systems, storing metadata that can be subpoenaed.
- Policy logic: “Accountability through traceability”; technical reality: no longer end-to-end.

EU’s #chatcontrol: Client-side scanning

The EU continues to test the limits of E2EE with “child safety” proposals.

- EU CSAM Regulation (ChatControl): client-side scanning by design.
- Fundamental rights concerns: violates privacy and confidentiality of communications (Art. 7–8 CFR).
- Status: 2025—extremely close margin of defeat under the Danish presidency;
  - Opposition from DPAs and technologists.
  - Germany was the deciding State, standing aside ahead of the most recent parliamentary session.
- Not going away anytime soon.

#chatcontrol the next generation

Denmark’s new proposal:

- Removes mandated scanning in encrypted environments (voluntary scanning is allowed to continue)
- For U16 it restricts
  - Downloading certain apps (WhatsApp, Telegram, Twitter, etc.)
  - Use of anonymous email or messenger accounts.

Other Europe: Sweden

Sweden’s new intelligence law raises backdoor risks through data-retention and lawful access.

- 2024 legal reforms expand interception powers for domestic intelligence.
- Pressure on service providers to “enable access” may implicate encryption.
- Debate over neutrality of Swedish telecom infrastructure operators.
- Signal has threatened to leave the country if subpoenaed.

Other Europe: France

National security framing used to justify device-level access.

- We have been here before– PEARG @ IETF 117
- 2025: Proposed “Digital Security Law” empowers interior ministry to compel on-device scanning.
  - Political rhetoric links encryption to “darknets” and terrorism.
  - Strong civil-society and CNIL (data protection authority) objections.

India: Traceability

India remains the most significant Asian threat to encryption.

- IT Rules (2021) require traceability; undermines E2EE metadata integrity.
- Draft Digital India Act (2024) may codify government access mechanisms.
- WhatsApp vs. Indian Government case still pending.
- Rhetoric is currently around crime, particularly drugs.

Canada: Link tracking

Canada has had a parade of bills risking embedding scanning obligations.

- Bill C-18: Online News Act compels content scanning.
- Bill C-63: Online Harms Act creates duty to mitigate harms but risks proactive scanning.
- Bill C-2: Strong Borders Act, Parts 14 and 15 provision “lawful access” to private information without a warrant and force services to install “technical capabilities” to access encrypted communications and sensitive data
- Civil liberties and technical communities raising E2EE alarms.

Future work: Technical

- E2EE even more ubiquitous
  - MLS in GSMA Open Gateway and RCS
  - MLS in ActivityPub for federated social media direct messaging
- And interoperable
  - Cross-platform, E2EE messaging interoperability.
- Clear and present guardrails around AI integrations

Future work: Policy advocacy

- Follow globalencryption.org
- Acute pressure to keep organizing in Europe especially
  - Bring in vast numbers of community-specific civil society groups
  - Let’s not let #chatcontrol disenfranchise youth from using the best privacy and security tools out there!
- Leverage failure
  - CALEA led to Salt Typhoon

Resources

- 2021 UCL project on “An evaluation framework for encryption policies" https://blogs.ucl.ac.uk/steapp/2021/12/09/encryption-pros-cons-a-balancing-act
- 2025 UCL project on “Government interventions into Encrypted Communications" https://isoc.box.com/s/6q1yhk71wybb01yqq2xlu9pmpj6ftfqa
- 2025 NYU+Cornell report on “How To Think About End-To-End Encryption and AI: Training, Processing, Disclosure, and Consent” https://eprint.iacr.org/2024/2086