11 September 2025

# Chat Control Cyprus Briefing

Internet Society

Global Encryption Coalition

Callum Voge voge@isoc.org

# Policy tensions with encryption

- Law enforcement wants access to devices and online platforms (encryption as a barrier)
- National Security wants protection from cyber attacks and espionage (encryption benefits)
- Consumers want control – protection  from hacking and attack (encryption benefits)
- Companies will always want to sell products that consumers want (encryption benefits)

# EU Child Sexual Abuse Regulation

- 2022 Proposal
- Good intention:
  - Reduce circulation of child sexual abuse material (CS
- Flawed approach:
  - Detection orders: providers must be able to identify, detect, and hand over evidence of CSAM
  - No exception for encrypted messaging
  - Result: providers pressured to either remove encryption or undermine encryption
  - Client-side scanning (upload moderation) pointed to as solution

# Client-side Scanning

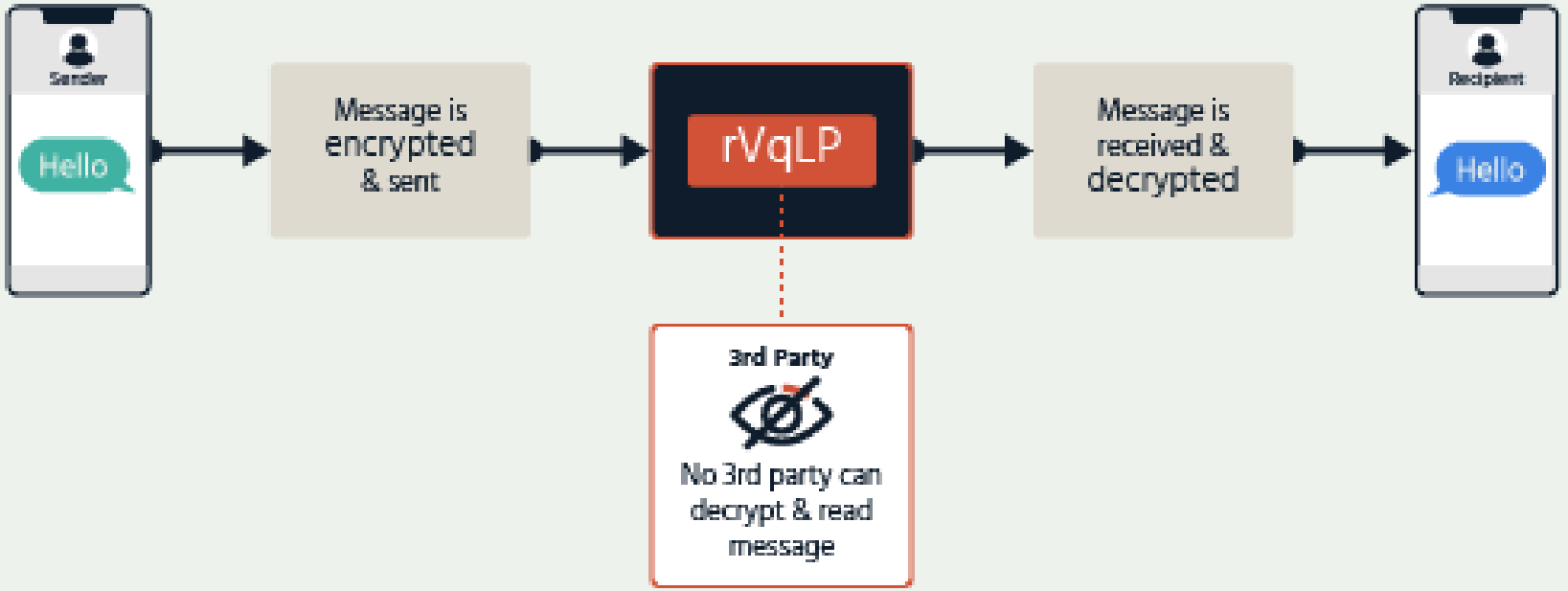
*Provider obliged to scan for content on user devices*

How it works:

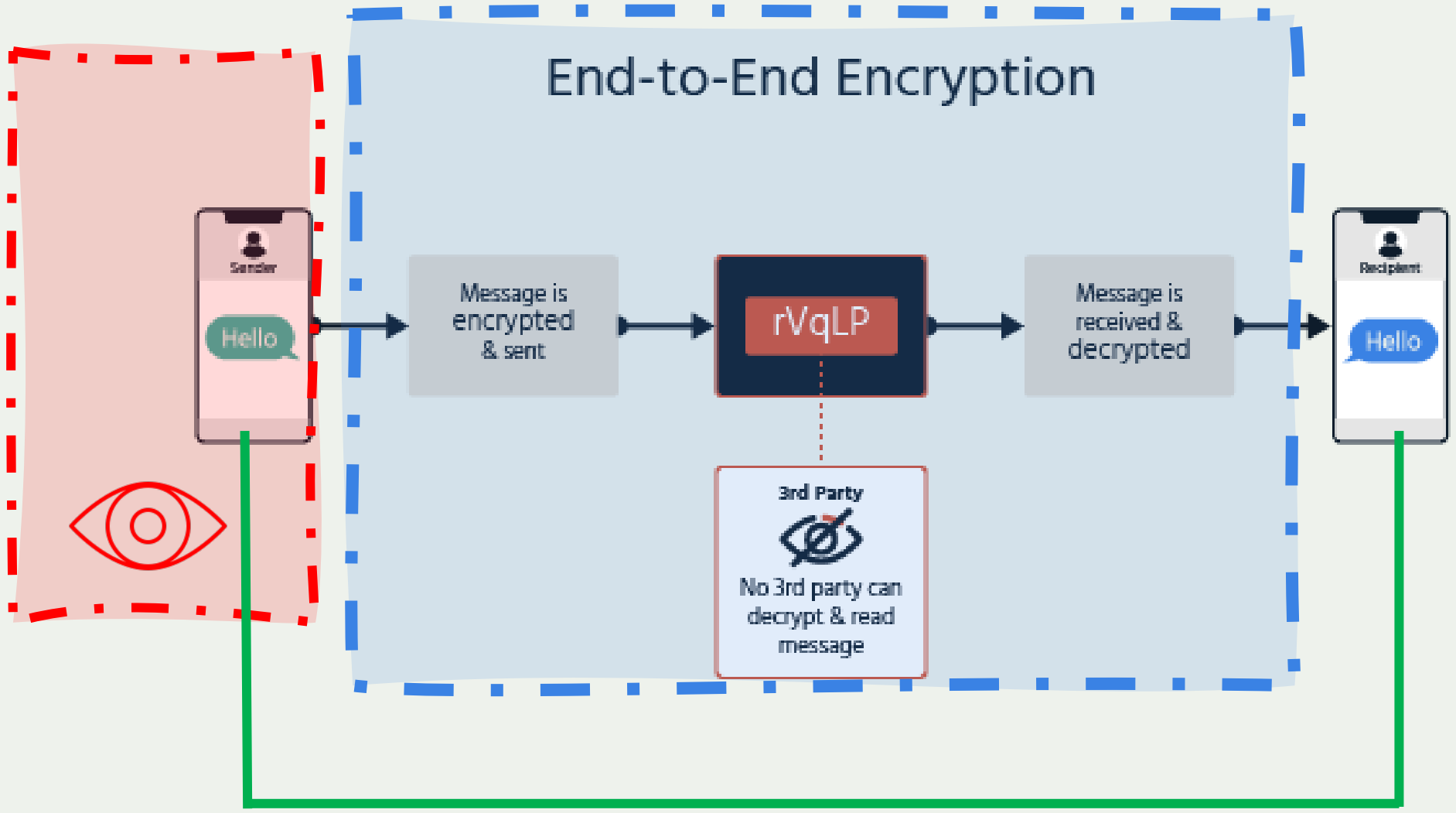
- Scanning happens on device (the client)
- Scanning results either processed on-device or off-device
- Hashes are created for scanning results
- Hashes compared against database of restricted content

# E2EE

## End-to-End Encryption



# CLIENT-SIDE SCANNING (IN E2EE)



# EU Child Sexual Abuse Regulation

European Commission

!

Original proposal – encryption threatened

European Parliament

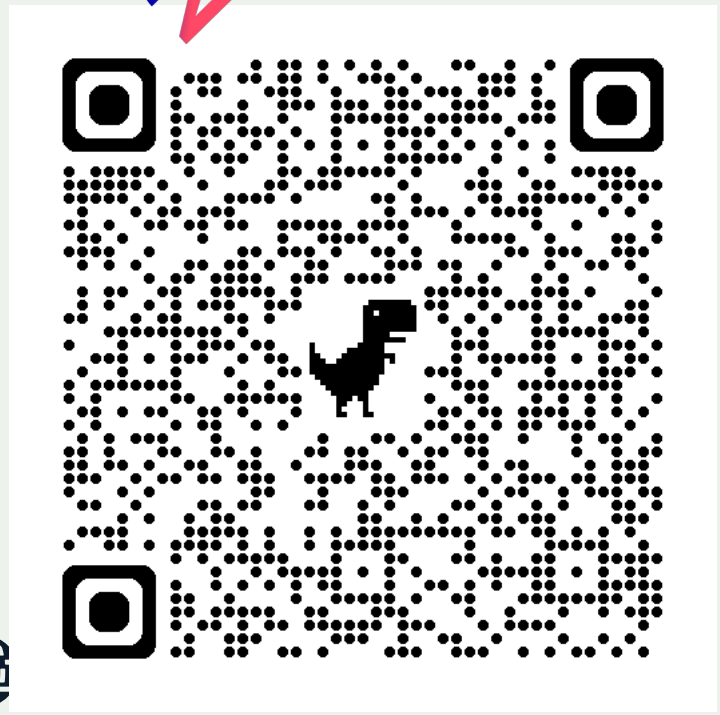
Private messaging removed from scope

?

European Council
Council of the European Union

Known and uknown CSAM
Encryption messaging still in scope

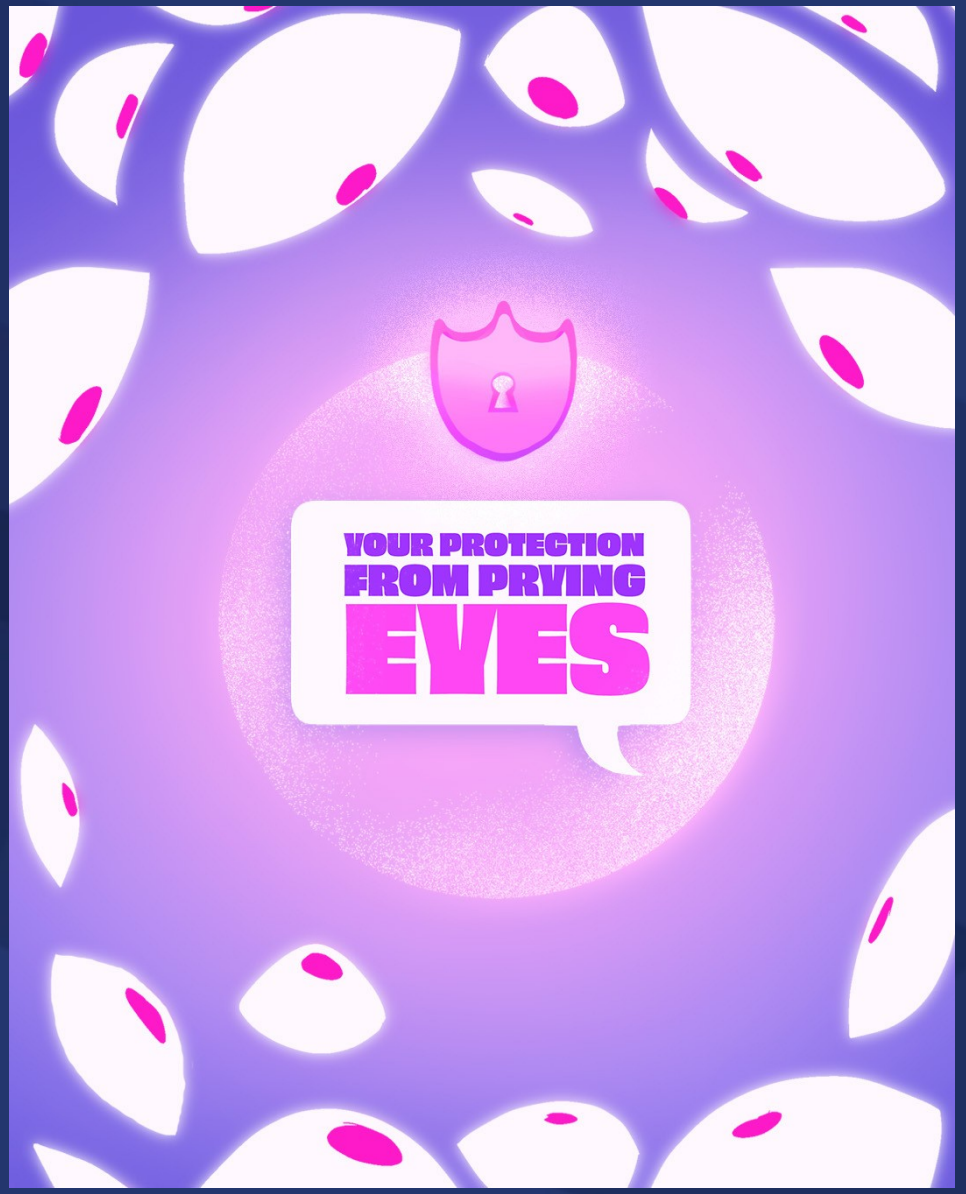
# EU Council text (Danish Text - October 2024)



<u>Global Encryption Coalition Steering Committee position</u>

- Mandated scanning
  - For both known and unknown CSAM
  - Technologies like client-side scanning
  - AI used in the case of unknown CSA
  - Surveillance of users without proven link to CSA crime

- On Encryption:
  - Narrow definition to protect ONLY “data in transit protected by means of encryption”
  - Require providers to undermine E2EE




- Mass scanning impact on rights:
  - surveillance of users without proven link to CSA crime
  - privacy risks and threat to exercise of human rights in digital space
  - government abuse – scanning for other types of material (scope creep)

- Efficacy:
  - Criminals can easily circumvent scanning, general public cannot (change file type, change bits in image)
  - False sense of security.
- Security:
  - Third party attacks on scanning system
  - Vulnerability in every device – attractive to criminals and hostile state actors


**Belgium:**

Mandated scanning: known and uknown CSAM


**Hungary:**

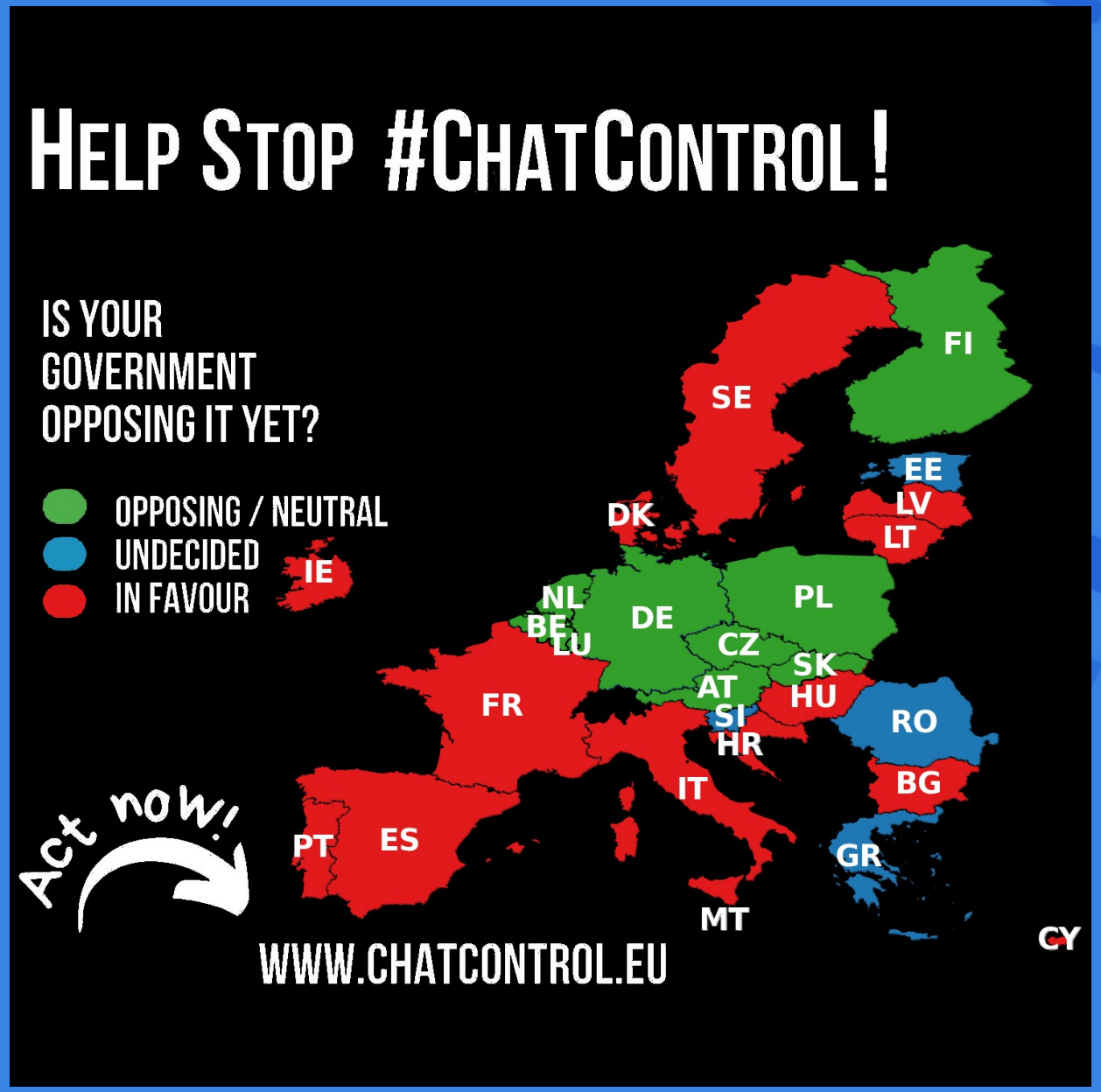
Mandated scanning: known CSAM only


**Poland:**

No mandated scanning in E2EE


**Denmark:**

Mandated scanning: known and uknown CSAM




# Council of the EU

**BLOCKING GROUP:**

- **Opposing Member States:** Poland, Germany, the Netherlands, Belgium, Luxembourg, Austria, Czechia, Finland, Slovakia.
- **Undecided Member States:** Romania, Estonia, Greece

# Cyprus takes over Presidency in January 2026

**Breaking encryption** is like tampering with an envelope while it transits through a post office. **Client-side scanning** is like reading the letter as it is being written.

In client-side scanning, the envelope is not tampered with, but the result is the same–the confidentiality agreement is violated.

# Thank you.

Internet Society
encryption@isoc..org

Rue Vallin 2
CH-1201 Geneva
Switzerland

11710 Plaza America
Drive Suite 400
Reston, VA 20190, USA

Rambla Republica de Mexico
6125
11000 Montevideo,
Uruguay

66 Centrepoint Drive
Nepean, Ontario, K2G 6J5
Canada

Science Park 400
1098 XH Amsterdam
Netherlands

3 Temasek Avenue,
Level 21
Centennial Tower
Singapore 039190

internetsociety.org
@internetsociety

# Security risks with Client-side scanning

PROCESSING ON DEVICE:

- Increased attack surface – reverse engineering
  - Circumvention
  - Criminal exploitation of scanning

PROCESSING OFF DEVICE:

- Attackers interfere with alerts sent between devices and server

Perceptual hashing:

- Security of multiple databases
  - Attackers could flood with false positives
  - Attackers introduce unauthorized material for scanning (i.e. facial recognition)

**Internet Society Analysis**