

# ChatControl 2.0: Breaking Private Communications

*Technical implications and expert assessments*

Marios Isaakidis, [marios@101.cy](mailto:marios@101.cy)



# What is Chat Control?

## EU Proposal to Scan All Private Messages

### The Regulation Would:




- Scan every message before you send it
- Check every photo you share
- Monitor all private communications
- Apply to all EU citizens (450 million people)



**Goal:** Detect child sexual abuse material (CSAM)

**Method:** Automatic client-sidescanning using AI technology

# How Your Messages Work Today

## End-to-End Encryption Protects Privacy

YOU → [Lock ] → [Send ] → [Unlock ] → FRIEND

 Your key  Friend's key

### Current Protection:

- Only you and your friend can read messages
- Even WhatsApp/Signal cannot see content
- Messages are encrypted before sending
- Confidentiality is protected by cryptography

# How Chat Control Would Change This

## Government Scanner Added to Every App

YOU → [Scanner 🔍] → [Lock 🔒] → [Send 📧] → FRIEND  
Check first      Then encrypt      Finally send


### New Process:

- AI scans content before encryption
- Suspicious content reported to authorities
- Every message checked automatically

# The Technical Methods

YOUR PHOTO/FILE




[Hash Check 




[AI Analysis 



[URL Check 



[Report/Allow 

# Expert Assessment: It Cannot Work

## 638 Scientists from 35 Countries Warn

### Technical Problems:

- "Not feasible to detect CSAM for hundreds of millions of users with acceptable accuracy"
- "Changing a few bits in an image bypasses detection"
- "No machine-learning algorithm can perform without large errors"
- "URL redirection makes detection notoriously unsolvable"

Source: [\*Scientists' Open Letter\*](#)

# The False Positive Problem

## When AI Gets It Wrong

### Real-World Examples:

- Family beach photos flagged as suspicious
- Medical discussions about children reported
- Art and educational content blocked
- Private jokes misunderstood as threats

### Impact:

- Up to 80% of alerts are false alarms
- Innocent people investigated by police
- Resources wasted on non-crimes

# Security Risks

## Breaking Encryption Creates New Vulnerabilities

### What Experts Warn:

- "On-device detection undermines end-to-end encryption protections"
- Creates backdoors that hackers can exploit
- Exposes financial, medical, and private data
- Makes everyone less secure online



# Who Gets Exempted?

## Exemptions For:

- Intelligence agencies
- Police communications
- Military personnel
- EU government officials

**Question: If it's safe, why exempt officials?**

# Official EU Assessment

## Data Protection Authorities Oppose It

### EDPB-EDPS Joint Opinion:

- "Disproportionate interference with fundamental rights"
- "Generalized and indiscriminate scanning"
- "Violates EU Charter Articles 7 & 8"
- "Unlikely to survive in court"

**EU's own legal experts say the proposal violates fundamental rights**

# The Bigger Picture

## Function Creep: Today CSAM, Tomorrow Everything

Current Scope	→	Future Expansion
Photos	→	All messages
CSAM	→	Political content
Children	→	Any crime
EU only	→	Global precedent

### Technical Reality:

- Scanner can be easily reconfigured
- No technical limits on expansion
- Creates infrastructure for mass surveillance
- Sets dangerous global precedent

# The Bottom Line

## Expert Consensus is Clear

### Technical Assessment:

- The technology cannot work reliably
- Easy for criminals to bypass
- Creates more problems than it solves
- Violates fundamental rights

*"This proposal completely undermines the security and privacy protections essential to protect digital society"*

# Learn More and Take Action

## Resources and Information

### Technical Details:

- [Scientists' Open Letter](#)

### Current Status and Action:

- [Fight Chat Control](#)
- Contact your representatives
- Stay informed about developments

**The decision affects all 450 million EU citizens**