OpenSSL CONFERENCE

Privacy is NOT the Enemy!

What law enforcement misunderstands & what cryptographers can do about it.

Katrina Khanta, D.Sc.
Cybersecurity Professional
[Independent Research]

Disclaimer

The research presented here is my own independent work, conducted in my personal capacity and outside the scope of my employment. The views, analyses, and conclusions expressed are solely mine and do **not** represent those of my employer or its affiliates.

This work was **not** commissioned, funded, reviewed, or endorsed by my employer, and I did **not** use any of its resources, data, or confidential information in preparing it. Nothing in this presentation should be taken as an official statement or position of my employer.

OpenSSL CONFERENCE

Agenda

1. Understanding this problem
2. Why privacy & E2EE matter
3. When the “good guys only” access fails
4. What works without breaking E2EE
5. A future for Privacy Enhancing Cryptography (PEC)
6. Cryptographers at the table

14.10.2026

OpenSSL CONFERENCE

Threat actors targeting children in immersive online environments

What makes these platforms ideal for bad actors to groom children?

14.10.2026

- Persistent relationships
- Normalizing communication (voice & text)
- Gift economies
- Age ambiguity
- Platform Fragmentation

The Grooming Funnel in Gaming

Target

Scout games frequented by minors. Identify vulnerable players (alone, struggling, seeking help).

Engage

Help with gameplay, give gifts, offer to 'carry.' Build a sense of debt and loyalty.

Trust

Position self as the best friend. Encourage secrecy. 'Don't tell your parents about me

Isolate

Move to private channels. Separate the child from peer support networks.

Exploit

Escalation - sexual content/coercion/meeting in-person

OpenSSL CONFERENCE

Platform Migration

Predators deliberately move off monitored platforms

In-Game Chat

Initial contact (often monitored)

→

Discord / Console DMs

E2EE available (opt-in; oversight varies)

→

WhatsApp / Telegram

WhatsApp: E2EE default; opt-in for backups
Telegram: E2EE opt-in

→

Signal / Wickr

E2EE + limited metadata by design (hardest to trace)

KEY CHALLENGE

By the time a case reaches detectives, the conversation trail has often moved across 3–4 platforms, each with different data retention policies, legal thresholds, and response timelines.

States with Highest Number of CyberTips

According to the National Center for Missing & Exploited Children (NCMEC)'s 2025 Annual CyberTip report:

Grand Total: 1,908,380

California – 238,572

Florida – 126,256

Georgia – 82,121

Illinois – 68,115

New York – 96,195

North Carolina – 69,807

Texas – 234,518

OpenSSL CONFERENCE

Cryptographic Foundation: FIPS 140-3 & CMVP

Before discussing E2EE is, it helps to understand how cryptographic implementations are validated

FIPS 140-3 & The CMVP

- FIPS 140-3 is the U.S. federal standard for validated cryptographic modules
- CMVP is jointly administered by NIST and Canada's CCCS, giving it international scope across Five Eyes and allied governments.
- A "module" is a specific validated implementation, not just an algorithm. This infrastructure supports security across financial systems, government communications, healthcare, and consumer platforms.

Why It Matters Here

- When policymakers propose "breaking encryption," they're effectively proposing to undermine this validation framework, the assurance layer that makes trust in any platform's security claims possible.

***OpenSSL has a FIPS certificate!**

Defining End to End Encryption

E2EE provides confidentiality such that only the defined 'ends-set' E (the intended communication endpoints) can access plaintext. The central property is endness: the system must be clear and honest about who the ends are, and any potential changes to that set over time." - Hale & Komlo (2022)

The 'ends' must be explicitly defined

- If a platform, service provider, or third-party module retains key access, the system is not E2EE to the user, regardless of marketing claims. Key access defines the ends.

CSS & backdoors break endness

- Client-side scanning inserts a third party into the ends-set. Hale & Komlo's (Example 3.3) demonstrates that PSI and homomorphic approaches when applied to message content face this same structural problem.

“If you have nothing to hide, you have nothing to fear”

A backdoor for "good guys" is still a backdoor

- **This mechanism is a vulnerability exploitable by bad actors**
- **Legitimate access can still be abused (surveillance technology)**

14.10.2026

What works without breaking E2EE?

Platform design
Default-off stranger DMs, opt-in friends, age-appropriate defaults

Behavioral signals
Contact graphs, rapid minor-account growth, off-platform pushes, gift flows

Better reporting
Actionable CyberTips; reports preserved 1 year (REPORT Act)

Capacity
ICAC funding, undercover operations, faster EDRs

Where Privacy Enhancing Cryptography (PEC) fits

Content path: untouched

Identifiers and metadata only

Private Set Intersection (PSI)
Multi-Party Computation (MPC)
Zero Knowledge Proof (ZKP)
Fully Homomorphic Encryption (FHE)

NIST is working on standardizing PEC, **OpenSSL** would likely implement upcoming NIST standards~!

NIST groundwork for standardization (IR 8214C, Jan 2026).

Narrowing the Privacy Dilemma with PEC

Tool	ICAC use	Financial-crime use	Limits
PSI	Match account identifiers vs. known-offender lists across platforms, revealing neither list	Banks/FIU find shared suspects without sharing customer lists	Identifiers only; on content it is CSS
MPC	Platforms jointly compute cross-platform risk; only a threshold result is revealed	Multi-bank analysis of layering and mule networks	Needs data standards, legal basis, coordination
ZKP	Prove age category without identity; prove policy or disclosure matched scope	Prove KYC/sanctions compliance without exposing data	Credential trust root; immature standards
FHE	Aggregate analytics on encrypted metadata	Shared fraud scoring on encrypted features	Expensive; key holder defines the ends

Private Set Intersection (PSI)
Multi-Party Computation (MPC)
Zero Knowledge Proof (ZKP)
Fully Homomorphic Encryption (FHE)

Example: Cross-platform repeat offender

Platform A bans an adult account

NCMEC/IWF & Platform B run PSI on identifiers

.

Only matches are revealed

+

Platform B applies protective defaults

Threshold of reports triggers legal process

Importance of Cryptographers at the Table

- Comment on NIST drafts and calls
- Technical reviews before legislation
- Attend ICAC and law-enforcement Conferences
- Publish policymaker-readable threat models
- Shape standards for PEC

Key takeaways

- Privacy is not the enemy; "nothing to hide" misunderstands what it protects
- "Good guys only" access fails two ways: exploited by others (backdoors) and abused by insiders (i.e., surveillance tech)
- Design before encryption; apply PEC to identifiers and metadata
- Cryptographers belong in policy and development decisions

We should not have to choose between privacy and safety. The choice is between putting in the extra effort to maintain both or taking shortcuts that make everyone less safe.

Privacy is a fundamental human right!

References

Cromwell, B. (2026). Government-imposed Backdoors Make Security Much Worse, Not Better. https://cromwell-intl.com/cybersecurity/backdoors.html
Brandão, L. & Peralta, R. (2021) Privacy-Enhancing Cryptography to Complement Differential Privacy. https://www.nist.gov/blogs/cybersecurity-insights/privacy-enhancing-cryptography-complement-differential-privacy
Hale, B. & Komlo, C. (2022). On End-to-End Encryption. IACR Cryptology ePrint Archive. https://eprint.iacr.org/2022/449
Institute of Justice. (2026). The IJ Database of ALPR Abuse. https://ij.org/the-ij-database-of-alpr-abuse/
Khanta, K. (2024) Protecting the Innocent: Safeguarding Children in Immersive Online Gaming Environments. https://www.proquest.com/docview/3158293914?sourcetype=Dissertations
National Center for Missing & Exploited Children (2026). 2025 Annual Reports by State. https://www.missingkids.org/content/dam/missingkids/pdfs/2025-reports-by-state.pdf
NIST. CMVP. https://www.csrc.nist.gov/projects/cryptographic-module-validation-program
NIST. Groundwork for Standardization (IR 8214C). https://csrc.nist.gov/news/2026/nist-and-multi-party-threshold-schemes
NIST. PEC Project (Brandão). https://www.csrc.nist.gov/Projects/pec.
The Washington Post. (2026). How Rogue Officers Turned a Nationwide Camera Network into a Tool for Stalking https://www.washingtonpost.com/technology/2026/08/02/how-police-officers-used-vast-network-cameras-spy-their-exes/
Velez, R. & POGO (2024). Agenda Illustration. https://www.pogo.org/analyses/we-built-a-surveillance-state-what-now