



Credits: After Skool

The Privacy Delusion

**In the Age of Cyber
Surveillance
Evgenios Anastasiadis,
Bridgefest III 2026**

How Dystopia Became Reality

FICTION PREDICTED. REALITY CONFIRMED.



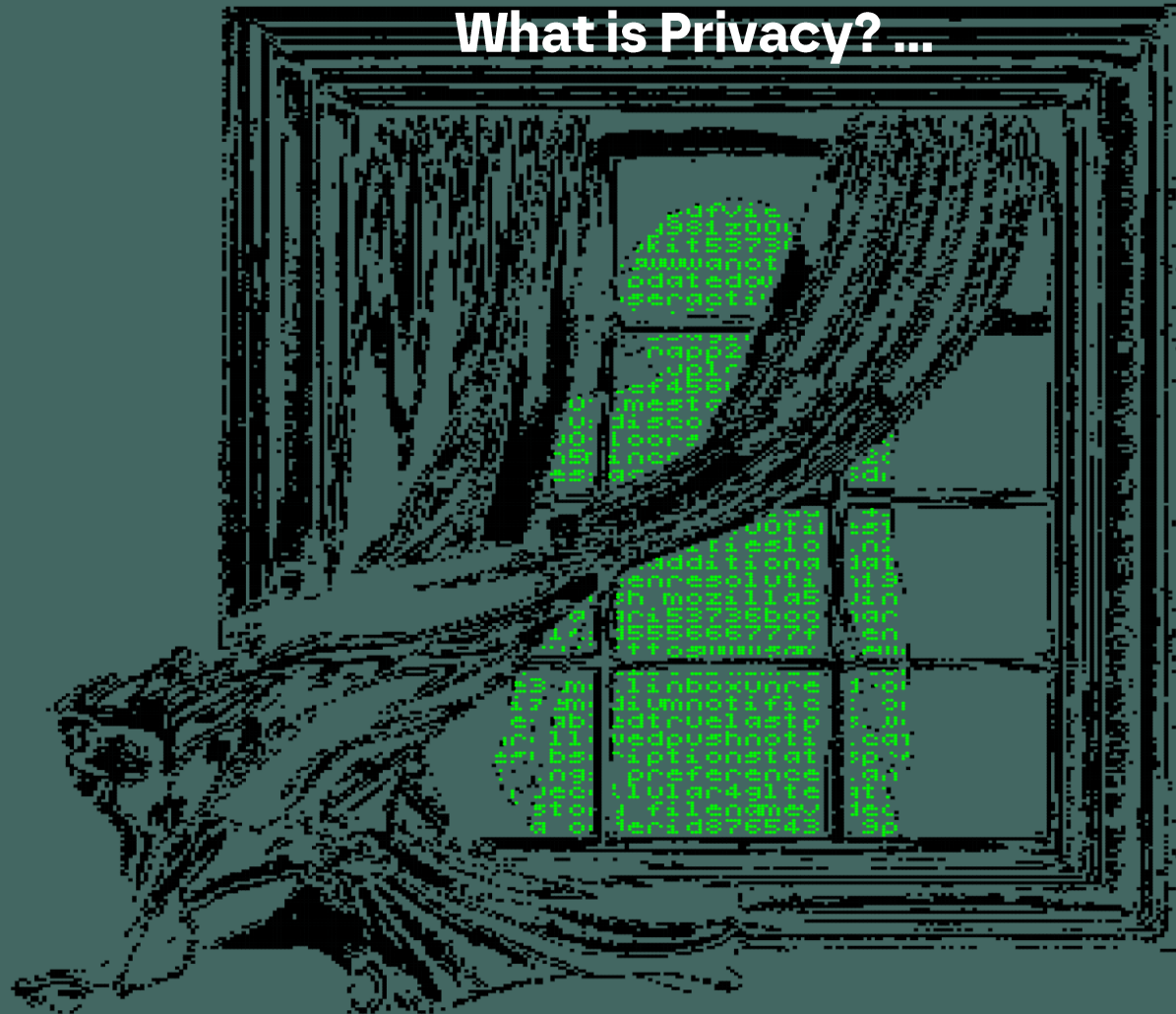
\$ whoami

Penetration Tester

Presented at Bridgefest I & II

First non-technical presentation (as always, bare with me 😊)

What is Privacy? ...



“Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, to what extent information about them is communicated to others.”

“each individual is continually engaged in a personal adjustment process in which he/she balances the desire for privacy with the desire for disclosure and communication”

[as]

I got nothing to hide!

Books That Warned Us



Nineteen Eighty-Four

George Orwell · 1949

Telescreens in every home.
Thoughtcrime punished before
action. The Ministry of Truth
rewriting history in real time. Big
Brother always watching.



Brave New World

Aldous Huxley · 1932

Citizens engineered for compliance.
Privacy a crime against stability.
Distraction as a control mechanism.
Individuality dissolved by design.



We

Yevgeny Zamyatin · 1924

Glass walls — no privacy anywhere.
Citizens numbered, not named. The
Benefactor surveils all. Dissent
pathologized as mental illness.

These books were written **77–102 years ago**. None of their authors had a smartphone, a social media account, or a smart speaker.
They saw it anyway.

Orwell's 1984 · Confirmed

Big Brother Is Now a Corporation

Orwell imagined the state watching. Reality is far more insidious — **we paid for the cameras ourselves.**

Telescreens → Smartphones

In 1984, the Party installed telescreens. Today, **8.9 billion smartphones** exist — devices people queued to buy that track location, record audio, profile behavior and report it to 400+ companies 24/7.

Thoughtcrime → Behavioral AI

Meta, Google, and Amazon build models predicting your next purchase, political lean, and emotional state — often **before you consciously decide**. Cambridge Analytica used this to manipulate **87 million voters** (2018).

Ministry of Truth → Platform Control

The UK Online Safety Act (2023) empowers Ofcom to demand backdoors in end-to-end encryption. A private regulator with power to mandate content removal — no vote required.

Room 101 → NSA Section 702

Snowden (2013) confirmed PRISM: the NSA had direct server access at Google, Apple, Facebook, Microsoft. Section 702 was reauthorized in 2024 — warrantless surveillance of Americans' international communications continues legally.

Pegasus: The State's Telescreens

NSO Group's Pegasus spyware — sold exclusively to governments — is the most documented case of state-run surveillance against civilians in the digital age.

Scale — WhatsApp Lawsuit (2025)

A court exhibit (April 2025) revealed **1,223 victims in 51 countries** targeted in just a 2-month campaign in 2019. Mexico: 456, India: 100, Bahrain: 82 — including journalists, lawyers and activists.

Inside the EU (2024)

Pegasus found on devices of exiled journalists in **Latvia, Lithuania, and Poland**. Including Maria Epifanova (Russia, infected Aug 2020) and Evgeniy Erlich (infected while vacationing in Austria, Nov 2022).

Jordan Investigation (2024)

Access Now + Citizen Lab found **35 confirmed Pegasus victims** in Jordan including Human Rights Watch staff, OCCRP journalists, and civil society lawyers — targeted between 2020–2023.

Togo — Journalists on Trial

RSF (Reporters Without Borders) confirmed Pegasus on phones of two Togolese journalists **actively standing trial** in a government-brought defamation case. Evidence gathered by the spyware they were being watched with.

Pegasus requires **zero clicks** to install. It silently enables mic, camera, messages, and GPS. Orwell called it a telescreen. NSO Group calls it a "lawful interception tool."

Phone spyware scandal in Greece moves to court as critics claim cover-up

24 September 2025

Share

Save

 Add BBC as preferred

Kostas Koukoumakas in Athens and Kostas Kallergis in Brussels



Chat Control — Scanning Your Messages by Law

The European Commission's "Chat Control" proposal is the most ambitious attempt by a democratic government to break end-to-end encryption — using child safety and national security as cover.

What Was Proposed

Mandatory scanning of **all private messages** — including end-to-end encrypted conversations on Signal, WhatsApp, iMessage. Detection orders to compare your chats against government databases. EU officials even suggested **AI to predict who might commit abuse** — pre-crime.

Who Opposed It

The EDPS (EU's own data protection supervisor), EFF, EDRI, cybersecurity experts, Signal, Apple, and multiple EU member states. All warned: breaking encryption means breaking it for **everyone** — including those the law claims to protect.

Timeline: A Multi-Year Battle

- **2022** — Commission proposes mandatory scanning
- **2024** — 4th Council term ends without agreement; proposal withdrawn for lack of majority
- **Dec 2025** — Council agrees new position: mandatory encryption scanning removed, "voluntary" scanning remains
- **Apr 2026** — EU Parliament votes to **block voluntary scanning derogation** — a win, but the core bill is still alive in trilogue

The Orwell Connection

In 1984, the Party reads every message, monitors every private conversation. Chat Control's "detection orders" are **functionally identical** — except the justification here is child protection.. The technical result is the same: no private communication.

The EU (still) wants to scan your private messages and photos

The "Chat Control" proposal would legalise scanning of **all** private digital communications, including encrypted messages and photos. This threatens **fundamental privacy rights** and digital security for all EU citizens.

[Home](#) > [Press corner](#) > [Commission unveils ProtectEU – a new European Internal Security Strategy](#)Available languages: EnglishPRESS RELEASE | [Apr 1, 2025](#) | [Strasbourg](#) | [4 min read](#)

Commission unveils ProtectEU – a new European Internal Security Strategy

PAGE CONTENTS

- [Top](#)
- [Quote\(s\)](#)
- [Related media](#)
- [Related topics](#)
- [Print friendly pdf](#)
- [Contacts for media](#)

Today, the European Commission is presenting **ProtectEU – a European Internal Security Strategy** to support Member States and bolster the EU's ability to guarantee security for its citizens. The strategy sets out an ambitious vision and workplan for the years to come, with a sharper legal toolbox, increased information sharing and deeper cooperation.

In a changed security environment and an evolving geopolitical landscape, where hybrid threats by hostile foreign states and state-sponsored actors are growing, where powerful organised crime networks are proliferating and criminals and terrorists are operating increasingly online, Europe needs to review its approach to internal security. Announced by President **von der Leyen** in the [political guidelines](#), the Strategy will upgrade the Union's response to new and traditional threats to internal security.

The Strategy aims to foster a change of culture on internal security, with a whole of society approach involving citizens, businesses, researchers and civil society. Security aspects will be mainstreamed in the development of new initiatives, and a new European internal security governance framework will support the implementation of the Strategy.



Photo taken from 39c3 Presentation: The Last of us – Fighting the EU Surveillance Law Apocalypse (Svea Windwehr, Chloe Berthelemy)

The UK Online Safety Act: A Blueprint for Repression

Passed October 2023, criminal offences in force from January 2024. The EFF calls it "a massive threat to online privacy, security and speech." Britain's government says it's making the internet "the safest place in the world."



Encryption Backdoors

Ofcom can compel platforms to scan end-to-end encrypted messages — effectively mandating backdoors. Signal and WhatsApp threatened to leave the UK rather than comply.



Mandatory Age Verification

Platforms must verify ages before showing "harmful" content — requiring real identity documents. Watching a YouTube video may soon require proving who you are to a private corporation.



Criminal Speech Liability

Up to **2 years imprisonment** for sending a message that causes "psychological harm amounting to serious distress" — defined by a regulator, not a court. Orwell called this Thoughtcrime.

European age verification app to keep children safe online

NEWS ARTICLE

15 April 2026 — Directorate-General for Communication — 1 min read



The EU's age verification app was hacked in two minutes

PRIVACY NEWS



Edward Komenda

Published on April 20, 2026

Share : [X](#) [Reddit](#) [Facebook](#) [LinkedIn](#) [Print](#)

The Surveillance State by Numbers

573

Million

CCTV cameras worldwide
(2024)

3,332

breaches

US data breaches in 2025 —
record high

€1.2B

fine

Meta GDPR fine 2023 —
largest ever

1,223

victims

Pegasus targets in 51
countries, 2 months



Location tracking

Your phone's location is sold to data brokers by default through ad frameworks. ICE (US Immigration) purchased location data from ordinary apps — including a prayer app — to track individuals without warrants.



Clearview AI

Scraped **50B+ images** from public web without consent. Sold to 3,100+ law enforcement agencies across 26 countries. Fined €20M in France, €7.5M in UK — still operating.



Meta Password Leak (2024)

Irish DPC fined Meta €91M in September 2024 after discovering **hundreds of millions of passwords** stored in unencrypted plaintext on internal servers — for years — without notifying users.

Instagram to remove end-to-end encryption for private messages in May

Meta's announcement comes after years of criticism from child safety groups over feature



The Soft Cage — You'll Love Your Chains

Huxley's insight was darker than Orwell's: oppression doesn't need force when people surrender privacy for pleasure.



Soma → Infinite Scroll

Huxley's soma numbed citizens into compliance. **4.9 billion** social media users average 2h 27min daily on dopamine-engineered feeds designed by behavioral psychologists to maximize time-on-site.



Conditioning → Consent Theatre

Children born into surveillance normalize it. **76 full working days** would be needed to read every ToS encountered in a year. "Consent" is legally obtained; meaningfully, it doesn't exist.



No Solitude → Always Online

Huxley abolished private thought. Average phone checks: **96 times/day**. Smart TVs, speakers, watches, and cars now create an unbroken surveillance mesh even at home.

The Glass City Is Real

In *We*, citizens lived in glass apartments — every movement visible. The most surveilled cities on Earth have made this literal.

Most Surveilled Cities (Cameras per 1,000 people)

Taiyuan, China	117 / 1K
Zhengzhou, China	46 / 1K
London, UK	8.9 / 1K
Singapore	7.6 / 1K
New York City, USA	4.2 / 1K

Facial Recognition: The Benefactor's Eye

China Social Credit System

1.4B citizens scored on behavior. Travel, finance, education restricted by algorithm. Zamyatin's "Numbers" made literal — your score is your identity.

UK Metropolitan Police Live FR

Real-time face-matching deployed on London streets. No parliamentary approval. Courts have not banned it. Citizens are scanned without knowledge or consent.

Clearview AI — Global Identification

50B+ scraped images. Any person photographed in public can now be identified in seconds. Used in 26 countries. Zamyatin imagined glass walls — this is faster.

Big Tech's Privacy Crimes — On Record

These aren't theories. These are confirmed violations with documented fines — the visible tip of a systemic iceberg.

Meta Facebook — EU-US Data Transfers

May 2023

€1.2 billion fine — largest GDPR fine ever. Meta illegally transferred EU users' Facebook data to US servers where it was accessible to NSA surveillance programs. Every European user affected.

Meta — Plaintext Password Storage

Sep 2024

€91 million fine. Hundreds of millions of user passwords stored in unencrypted plaintext on internal servers for years. Visible to all ~20,000 Meta employees. Users were never notified.

Meta Instagram — Children's Data

Sep 2022

€405 million fine. Children's phone numbers and email addresses made public by default through Instagram's Business Account feature. Meta processed children's data without valid legal basis.

Meta — Forced Ad Consent

Jan 2023

€390 million fine. Meta required users to accept personalized ads in ToS to use Facebook/Instagram/WhatsApp. "Consent" hidden in contract terms — not freely given, legally invalid.

Meta's total GDPR fines: **over €2.1 billion**. For a company with annual revenue over \$160B, this is a parking ticket. The surveillance continues.

Uber Accused Of Increasing Prices When User's Phone Battery Is Low: Report

However, Uber disputed that the payment is based on how much battery life is left in a phone. It further claimed that the app is unable to measure a user's battery.

Edited by: [Anoushka Sharma](#) | [World News](#) | Apr 14, 2023 13:19 pm IST ⓘ

Read Time: 3 mins

↪ Share



From Fiction to Confirmed Fact

1924–1949

Zamyatin's *We*, Huxley's *Brave New World*, Orwell's *1984*. Three separate authors, three separate countries, one shared vision: surveillance states that crush privacy and manufacture consent.

The Warnings

2013

NSA PRISM: direct access to Google, Apple, Facebook, Microsoft, Yahoo servers. The state telescreen was real, and had been operating for years. No one was prosecuted. The program continues under Section 702.

Snowden Confirms It All

2018

87 million Facebook profiles harvested. Used for micro-targeted political ads across the US and UK elections. Huxley's behavioral conditioning, industrialized and deployed for electoral manipulation.

Cambridge Analytica

2022–2026

EU Chat Control proposes mass message scanning. UK Online Safety Act creates backdoor mandates & criminal speech liability. NSA Section 702 reauthorized 2024. Pegasus used on EU soil. 573M cameras. It's not coming — it's here.

Laws Join the War on Privacy

May 2026

EU Chat Control still in trilogue. UK Online Safety Act enforcement begins. Record breach numbers. Pegasus confirmed in EU member states. The books are not predictions anymore — they are **documentation**.

Today



*Privacy is not something you lost.
It's something you were convinced
you never needed.*



Orwell was right about surveillance — wrong only about who runs it. Huxley was right about method — the cage is algorithmic and we decorated it. Zamyatin was right about glass walls — today's cameras are just smaller.

Orwell was right

About surveillance — corporations reached it before states did. Telescreens are iPhones. PRISM is Room 101.

Huxley was righter

The cage is dopaminergic. You chose it. Infinite scroll is soma. The "nothing to hide" mantra is soma for your reasoning.

Both are now law

Chat Control, the Online Safety Act, Section 702 — the fiction is codified. Governments read the books as manuals, not warnings.



They Told Us. We Didn't Listen.

The delusion is optional.
Awareness is the first act of resistance.



Thank you!

Evgenios Anastasiadis
Bridgefest III