Backdoors in your smartphones? How? Why? Not?

Aurélien Francillon, EURECOM

May 5th, THCon 2026

Aurélien Francillon

Professor in the security department at EURECOM

aurelien.francillon@eurecom.fr

https://www.s3.eurecom.fr/~aurel/

Working on security of embedded

Leading PEPR Cybersécurité project REV (France 2030), ANSSI scientific council

GDR Transversal Action on Information Security and Social Sciences & Humanities (Action transverse GDR Sécurité Informatique et SHS)

FRANCE 2030

EURECOM
Sophia Antipolis

Aurélien Francillon

Interaction of hardware/software/wireless communication

Notable projects in (embedded) software security:

- Avatar2: Framework for embedded firmware testing
- SymCC/SymQEMU : Fast concolic execution for code / binaries
- LibAFL-QEMU : Fuzzing from QEMU VMs

Wireless security/side channels:

- Screaming Channels: Side channels propagate over radio, and Bluetooth
- PhaseSCA : Exploiting information leakage on phase instead of amplitude

And I like backdoors ! But we will come back to this shortly.

TODOS

Mention references Otmar blog

- Eu expert group
- CCS Savage paper for offline
- Don’t say police

Add : Charlie Hebdo attacks, “black boxes”

- Law in 2015, status report ?

Structure:

- Backdoors
- Backdoor or front door ?
- If not a backdoor is it good ?
- Word on hdd backdoor / backdoor definitions ?

Why?

Why backdooring phones ?

Well this is quite obvious why ? We need to protect the society, against terrorism, child exploitation, organized crime… (hackers ?)

Since 2015. 270+ people killed in France because of terrorist attacks.

Drug trafficking or Child abuse definitely a large problem…

https://www.ifri.org/en/shedding-new-light-terrorism-france
https://en.wikipedia.org/wiki/List_of_terrorist_incidents_in_France

Why do we have this debate again ?

- Smartphones are everywhere
- Smartphones security is getting quite high !
  - Noticed Copy.fail vulnerability ?
  - => Android not vulnerable (SELinux policy)
- All our data, credentials, online activities are there
- Encrypted messaging is pervasive:
  - Signal, WhatsApp, etc.
  - Even SMS now RCS is End-to-End Encrypted (E2EE)

- And yes, criminals and terrorists use them, like us.
  - EncroChat, SkyECC, Anom …

Big Tech Google

Google says all group RCS chats are now fully end-to-end encrypted

Just make sure no one in your group has opted out before sharing any big secrets.

by Kris Holt • Aug. 8, 2023 4:03 pm EST

https://www.engadget.com/google-says-all-group-rcs-chats-are-now-fully-end-to-end-encrypted-200337049.html

Encryption

Apple beta introduces end-to-end encryption for RCS, enhances security features

February 17, 2026

Share

By SC Staff

(Credit: ink drop – stock.adobe.com)

Apple has begun testing end-to-end encryption (E2EE) for Rich Communication Services (RCS) messages in its latest developer beta of iOS and iPadOS. This move aims to bolster the security of communications between Apple devices, as reported by The Hacker News.

https://www.scworld.com/brief/apple-beta-introduces-end-to-end-encryption-for-rcs-enhances-security-features

How?

History of the “crypto wars” and “wiretapping”

Intercepting/Opening physical mail (since we write?) Caesar Cipher ? Older examples.

Phone wiretap / Lawful Interception (since phone was created?)

1955 scandal of illegal wiretapping in New York

DES in 70’s : NSA made sure the DES standard appeared before others did the standard, that the key length wasn’t too long (so NSA could brute force it), but wasn’t too vulnerable (so others couldn’t).

90’s the clipper chip : communication chip with escrow key

Black-Boxes (“Technique de l’algorithme”): algorithme

- Introduced in 2015 for fighting terrorism
- Extended for foreign influence (2021) and narcotraffic (2025)
- State council rejected both extensions, stating too many risks for individual liberties
- Planning to come back in LPM 2026

And failures

Greek mobile wiretap scandal (2005)

China hack of the USA telecom operators using Lawful intercept “Salty Typhoon” 2023/24

https://spectrum.ieee.org/the-athens-affair

https://www.commerce.senate.gov/2025/12/experts-agree-u-s-communications-networks-remain-vulnerable-following-salt-typhoon-hack

Digitization of society and surveillance

A lot of data is available everywhere, a lot more than 50 years ago !

Intelligence agencies collect a lot of data,

- public data, applications data, advertisement data

Searching a smartphone is more like a house search than a phone wiretap.

- House search requirements a lot more strict than phone wiretap

Who thinks that Lawful interceptions should not exist?

Telecom networks before v.s. Now

- Centralized on a telecom operator
  - Or a few well identified companies
  - They have to comply with the local laws
- Voice largely in clear
  - Encryption mobile: only for the wireless link
  - Maybe between telecom operators, but each has access to the data
- Only voice, limited exposure of personal life

- E2EE systems don’t trust
  - The network
  - The server
  - Open source …
- “Service provider” has nothing to share
  - Well some metadata is still data …
- Protocols security keeps on improving.
- Contains all your life digitized!

Which data ? Context in which to access to data?

Data at rest :

- Seized device: recovery of data from a phone: Forensics
- Cloud storage

In transit :

- Chat applications => Lawful Interceptions

In use:

- Trusted computing ? TEEs ?
- Exploits to exploit smartphones remotely
- Data on phones remotely?
- On device scanning ?

ChatControl : on device scanning

Massive on device scan of all pictures / media shared on messaging apps

Messaging apps/OS needs to scan content, build a perceptual hash

Compare the hash to a database

Not cryptographic hash (not robust to changes)

=> Doesn’t work

=> EU commission keeps on pushing this forward, and it keeps on failing to be voted (fortunately)

Perceptual hashes: Ideally

Images similaires → hashs égaux ou proches

acb0fdf52d424a1c498120b5 acbdfdf52d424a1c498120b5

Images différentes → hashs totalement différent

acb0fdf52d424a1c49812 0b5 8915b18199bbba561128 2e7b

Many attacks: collisions, evasion, injection

05287734eab66e5fecb908eb

Black-box Collision Attacks on Widely Deployed Perceptual Hash Functions

Diane Leblanc-Albarel

Bart Preneel

https://eprint.iacr.org/2024/1869

False positives Between 0.03% and 0.3%
750M Europeans
=> 1 pic/person/day: 225k to 2,25M false detections/day (without any attack)

False positives:
On the Cost-Effectiveness of Mass Surveillance
Javier Parra-Arnau,
Claude Castelluccia,
https://inria.hal.science/hal-01921899

White-Box Attacks on PhotoDNA

White-Box Attacks on PhotoDNA Perceptual Hash Function

Maxime Deryck, Diane Leblanc-Albarel and Bart Preneel

https://eprint.iacr.org/2026/486 March 2026 https://www.pseudodna.eu/

Reverse engineering and complete break of PhotoDNA, Forgery in seconds or minutes:

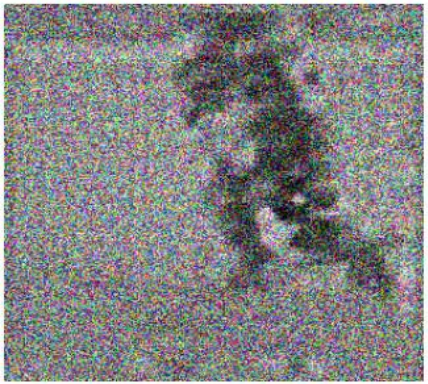
- False detections
- Injecting patterns to make the images match while they should not
- Modifying images to make them not match known CSAM while they should…
- Generate 2 images with same hash
- Generate image with null hash (all zeros…)

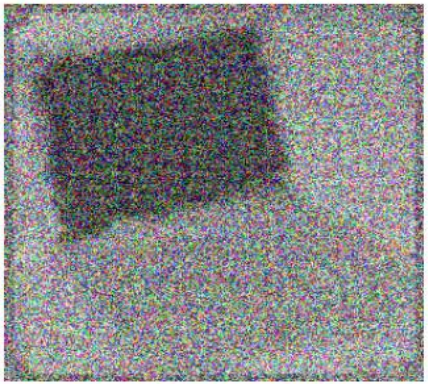
Exact collisions

(a) Original images

(b) Exact collision

Recovery from a hash value





Data in transport: Ghost / Lawful Intercept

Article 8 Ter from “Loi narcotraffic”: Mandate to send the data to police in case of lawful interception request (approved etc.).

“Protecting the cryptography”, not mass surveillance…

Unclear references to the “Ghost” :

- Adding one invisible participant to the (group) chat

Alternative propositions : send data in the clear before encryption

Was not included in the final law.

Cybersecurity & Tech Surveillance & Privacy

Principles for a More Informed Exceptional Access Debate

Ian Levy, Crispin Robinson | Thursday, November 29, 2018, 8:00 AM

This is part of a series of essays from the Crypto 2018 Workshop on Encryption and Surveillance.

In any discussion of cyber security, details matter.

https://www.lawfaremedia.org/article/principles-more-informed-exceptional-access-debate

NEWS & COMMENTARY

The 'Ghost User' Ploy to Break Encryption Won't Work

Jon Callas,
Senior Technology Fellow,
ACLU

July 23, 2019

Note: This is part one of a four-part series where security expert Jon Callas breaks down the fatal flaws of a recent proposal to add a secret user — the government — to our encrypted conversations.

Twenty-five years ago, the FBI decided it needed a surveillance system built into the nation's telephone network to enable it to listen to any conversation with the flip of a switch. Congress obliged by passing the Communication Assistance to Law

https://www.aclu.org/news/privacy-technology/ghost-user-ploy-break-encryption-wont-work

Hard questions !

How do we ensure that new access mechanisms do not weaken system security?

What guarantees ensure that the system is not easily by passable?

Shall we exclude police, government, military from it? (see later)

How should jurisdiction be handled, especially with international travel?

- I’m Iranian, buy a phone in US, move to France, China, Japan? Who should access it?
- If Europe makes this mandatory, and it gets implemented, China and Iran will also ask the access ?
- Give all your data every time you pass a border?

How to ~~backdoor an app~~ Enable Lawful Interception

Not many ways:

- Get an authorization mechanism
- Send the data to Law Enforcement
  - Or the key
  - Or add LE to a group chat
- Or Scan on device for something ?
- Or weaken the cryptography ?

Cryptography e.g., for E2EE chat is actually hard to get right, lots of vulnerabilities without the backdoor.

=> Adding backdoors will make it even harder to get right, so weaker

=> While at the same time impossible to force bad actors to use those platforms

=> Is a documented backdoor (law) still a backdoor ? Or a front door ?

Phone Forensics: making data accessible in a controlled way?

- Extracting data from phones, is difficult
  - Often requires very advanced attacks
  - Access keys, decrypt…
  - Phones are more and more hardened against faults and side channel
- Stefan Savage (paper CCS 18)

Lawful Device Access without Mass Surveillance Risk: A Technical Design Discussion

Stefan Savage
Department of Computer Science and Engineering
savage@cs.ucsd.edu

ABSTRACT

This paper proposes a systems-oriented design for supporting court-ordered data access to "locked" devices with system-encrypted

open the door to mass surveillance and inherently weaken security against other threats.[1]

Absent better solutions, the current state of affairs is one that

Not?

Chat Control is not Lawful Interception but mass surveillance

ChatControl:

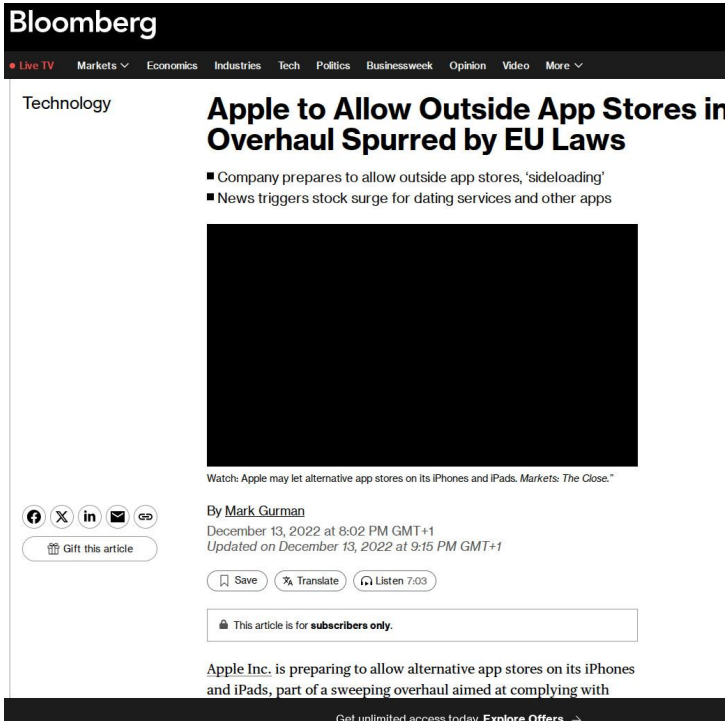
- The phone is scanning message contents before sent, before encryption
- On every phone
- Using local detection: perceptual hashes…

And ineffective ? How to ensure it is not too easy to bypass?

- Trivial to fork open source / side load
- Shall we forbid open source ?
- EU just guaranteed alternate installation sources on smartphones markets possible ?
- If some app is not available, on EU vendor market, side load etc…

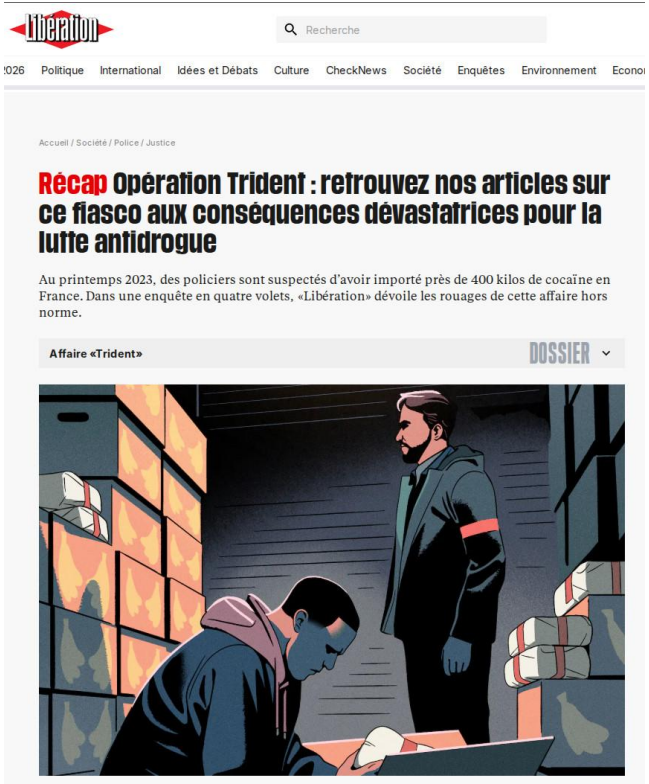
Among you: who would load a fork of Signal if LI access is added ?

- And you can sideload a version without the backdoor.



So shall we exclude the police from wiretap?

- Scandal of 450Kg of cocaine imported and distributed with help from police
  - No Cocaine or money recovered
- If there was a backdoor i bet they would not have used it.



More than this, policemen are humans and human security is difficult too…

Police behaving badly

Alice Hutchings
Director, Cambridge Cybercrime Centre
Department of Computer Science & Technology
University of Cambridge
Cambridge, UK
alice.hutchings@cl.cam.ac.uk

***Abstract*—Police officers and employees misusing access to police database now account for over half of all cybercrime prosecutions in the UK. The harms this can cause are considerable. Yet police continue to call for encryption to be weakened to allow for greater access to communication data.**

***Index Terms*—Cybercrime, policing, unauthorised access**

Some of the stories I come across in my research resemble movie plots. An encrypted messaging network and modified device provider is used by those involved in the illicit drug trade, murderers, gang violence, and other crimes for secure communication. A top secret law enforcement operation infiltrates the messaging service, leading to a huge amount of broiled in corruption, drugs, murder, and sex. They demonstrate the significant harms that can be caused, from the cost to witnesses, ongoing investigations, trust in the criminal justice system by the general public, and severing of trusted relationships with international authorities. Police employees have access to vast amounts of sensitive information, and this is vulnerable to misuse. This can include details of those who have had contact with the criminal justice systems, as witnesses, victims, suspects, and offenders.

Unfortunately, these examples are not isolated incidents. I maintain the Cambridge Computer Crime

Cybersécurité : Ce que l'on sait du piratage du ministère de l'Intérieur

Parmi les fichiers qui auraient pu être consultés figurent notamment le Traitement des Antécédents Judiciaires (TAJ) et le Fichier des Personnes Recherchées (FPR) – deux bases de données parmi les plus sensibles de l'appareil d'État. Le TAJ regroupe les informations issues d'enquêtes de police ou de gendarmerie, incluant les personnes mises en cause, victimes ou témoins, même sans condamnation. Le FPR contient quant à lui des signalements relatifs à des individus surveillés, recherchés ou visés par des mesures administratives ou judiciaires.

Trust ?

I first thought this was a scam :)

ANTS:

- the secure documents agency
- ID cards, passports, car registration…
- Face and fingers biometrics
- Can't change a biometric ID…

From	France Titres <no-reply@comm.ants.gouv.fr>
To	aurelien@francillon.net
Subject	Incident de sécurité
Date	Mon, 20 Apr 2026 15:15:01 +0200

France Titres
AGENCE NATIONALE DES TITRES SÉCURISÉS

Bonjour,

Le 15 avril dernier, l'agence nationale des titres sécurisés (ANTS) a eu connaissance d'un incident de sécurité sur son site.

Cette attaque a entraîné un accès non autorisé à certaines données personnelles associées à votre compte usager dont :

- les données relatives à votre état civil (nom et prénom) ;
- les identifiants de connexion (identifiant de compte et adresse mail) ;
- et d'autres données présentes uniquement dans certains comptes (adresse postale et numéro de téléphone).

ANTS leak.

Fortunately the most sensitive data not lost. But 11,7 millions accounts…

One of the most sensitive government infrastructure, by definition data from all citizens, biometrics, etc

Discovered because (one of?) the authors, a 15 years old tried to sell data on an underground forum…

I have a high respect for security people in the government, impressive profiles and skill level in many places.

- But this is not the problem!
- The problem is: if we create this access LI in all phones, how good are we going to be at protecting it?

https://www.lepoint.fr/societe/piratage-de-lants-ce-que-lon-sait-sur-breach-3d-le-hacker-de-15-ans-arrete-en-corse-6KEPSH26YBGMDJTCC7D5BSXX6Y/

Without Legal Intercept in phones? Exploit market…

Law Enforcement/Intelligence agencies buy forensics / exploits tools

- Extracting information from seized device
- Exploiting devices remotely

Tens of M€ / Year per country

Cellebrite 500M€ revenue / year

Funding exploit market, and who controls who gets to use what?

Who is to decide who should have access to what ?

Move to exploitation

market ?

Well known sovereignty issue…

THE TIMES OF ISRAEL

Italy, Israeli spyware firm cut ties after Rome accused of hacking critics' phones

Italian parliamentary committee says government used Paragon spyware with permission of prosecutors to counter illegal immigration, alleged terrorism, criminal activities

By GIUSEPPE FONTE and ALVISE ARMELLINI

9 June 2025, 9:11 pm

SHARE

Status in France : Loi Resillience (NIS2, DORA, REC)

Emergency procedure only 2 steps:

1) Senate : added “illegal for police force to impose backdoors”

(“Commission” Parliament approved the article in September)

2) Parliament (Assemblée nationale)

   Not put to the agenda…

Where are we now?

Chat control, 1 and 2?

ChatControl 1 : check for CSAM on cloud servers (e privacy directive workaround)

ChatControl 2 : check CSAM on devices, breaking E2EE

None for now are in place, for now (1 actually just expired)

Will they come back? I wouldn't be surprised …

Backdoors: Status in France

L'USINEDIGITALE

Intelligence artificielle | Cybersécurité | Big Tech | Robotique | Cloud

Accueil > Cybersécurité > Le récap' cyber

NIS 2 bloquée par l'obsession de la DGSI d'introduire des backdoors dans les messageries

Alice Vitard

Publié le 19 février 2026 à 14h00

Partager

Backdoors: Status in France

PIXELS • SÉCURITÉ INFORMATIQUE

Le gouvernement n'a pas renoncé à accéder au contenu des discussions sur les messageries chiffrées

Sébastien Lecornu a missionné le député Florent Boudié pour mener une réflexion sur des évolutions du droit qui permettraient de ménager aux enquêteurs et aux services de renseignements un accès aux communications chiffrées, sous certaines conditions.

Par Martin Untersinger
Publié le 22 janvier 2026 à 08h56, modifié le 22 janvier 2026 à 09h59 · Lecture 3 min.

Offrir l'article | Lire plus tard

Article réservé aux abonnés

Le gouvernement n'a pas renoncé à se ménager un accès aux discussions sur les messageries chiffrées telles que Signal ou WhatsApp. Par le biais d'un décret paru

Édition du jour
Daté du jeudi 12 mars

Le Premier Ministre

--81/26 SG

Paris, le 19 JAN. 2026

Monsieur le Président, cher Florent,

Le chiffrement de bout en bout *(end-to-end encryption)* contribue directement à la protection des données sensibles de leurs utilisateurs et à la protection de la vie privée de nos concitoyens. Pour autant, il peut également faire obstacle aux enquêtes portant sur des infractions graves ou visant à prévenir les atteintes aux intérêts fondamentaux de la Nation.

Cette situation illustre un véritable dilemme de politique publique : concilier la nécessité d'un accès légal et légitime aux communications dans le cadre du renseignement et des enquêtes judiciaires, avec l'impératif tout aussi fondamental de préserver la robustesse des technologies de communication utilisées quotidiennement par nos concitoyens, par les entreprises, par les opérateurs essentiels ou vitaux et par l'État lui-même.

Le Premier Ministre

--81/26 SG

Paris, le 19 JAN. 2026

Monsieur le Président, cher Florent,

Le chiffrement de bout en bout *(end-to-end encryption)* contribue directement à la protection des données sensibles de leurs utilisateurs et à la protection de la vie privée de nos concitoyens. Pour autant, il peut également faire obstacle aux enquêtes portant sur des infractions graves ou visant à prévenir les atteintes aux intérêts fondamentaux de la Nation.

Cette situation illustre un véritable dilemme de politique publique : concilier la nécessité d'un accès légal et légitime aux communications dans le cadre du renseignement et des enquêtes judiciaires, avec l'impératif tout aussi fondamental de préserver la robustesse des technologies de com s, par les opérate

Vous me remettrez vos travaux d'ici trois mois.

The report should be out soon, will it be public?

But 3 months to solve the problem was short ;)

In the meantime:

Sénat - Accueil / Travaux parlementaires / Office et délégations / Délégation parlementaire au renseignement / Chiffrement et algorithmes : la délégation renseignement apporte sa contribution

DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT

Chiffrement et algorithmes : la délégation parlementaire au renseignement apporte sa contribution

4 mai 2026

La délégation | Présentation | Composition | Rapports | Communiqués de presse | La CVFS

Sous la présidence de Muriel Jourda, sénateur, **la délégation parlementaire au renseignement a, depuis le début de l'année 2026, consacré ses travaux à l'évaluation du cadre juridique et de la mise en œuvre des techniques de renseignement, notamment la technique dite de l'« algorithme »**, et à **la problématique du chiffrement** au regard de la politique publique du renseignement.

Faisant usage des prérogatives qui lui sont reconnues par

Délégation parlementaire AU RENSEIGNEMENT

Communication de la délégation parlementaire au renseignement

Sous la présidence de Muriel Jourda, sénateur, **la délégation parlementaire au renseignement a, depuis le début de l'année 2026, consacré ses travaux à l'évaluation du cadre juridique et de la mise en œuvre des techniques de renseignement, notamment la technique dite de l'« algorithme »**, et à **la problématique du chiffrement**

Parliamentary Intelligence Oversight Delegation

- Argues for targeted access to encrypted communications
  - Would preserve against mass surveillance
- Claims such access may be technically feasible without generalized weakening
- Criticizes the anti-backdoor provision in the resilience bill as harmful to intelligence policy
- current encryption as a major operational obstacle for intelligence and justice.

Do not propose any solution, ignores that illegal activities won't comply with the "legal protocols", distributed, no central system.

Although this delegation was calling for a more open and clear debate, It would be interesting to hear.

So what would you do ?

Challenges:

How do we ensure that new access mechanisms do not weaken system security?

What guarantees ensure that the system is not easily by passable?

Shall we exclude police, government, military from it?

- Diplomats ? Intelligence agents ?
- This is not a rhetorical question, this was proposed in CSAM

How should jurisdiction be handled, especially with international travel?

Are solutions: Technical? Sociological? Political? Legal?

I think it is a society question, which needs multidisciplinary approach

In a democracy, we need an informed debate about it, researchers, hackers, associations need to brainstorm about this

Approach the problem critically.

Your turn,
Let's start the debate
(Q& A)

References and resources.

On peut accéder à votre smartphone à votre insu… à quelles conditions est-ce légal ?, The conversation, Aurélien Francillon, Noémie Véron

Détecter les contenus pédocriminels en ligne : quelles options techniques ? Quels risques pour la vie privée ?, The conversation, Aurélien Francillon, Diane Leblanc-Albarel, Francesca Musiani, Pierrick Philippe

“Vie privée ou sécurité : jusqu’où faut-il aller ?” AOC.media, Aurélien Francillon, Diane Leblanc-Albarel, Francesca Musiani et Pierrick Philippe

Otman Lendl Blog

White-Box Attacks on PhotoDNA Perceptual Hash Function *Maxime Deryck, Diane Leblanc-Albarel, Bart Preneel*

The 'Ghost User' Ploy to Break Encryption Won't Work Jon Callas