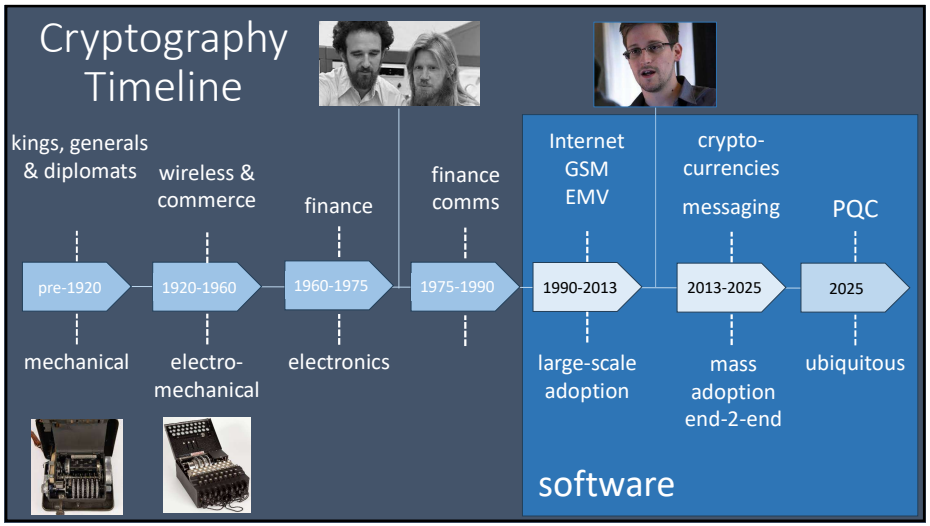

Cryptography policy and 50 years of crypto wars
Bart Preneel
firstname.lastname@esat.kuleuven.be
https://www.linkedin.com/in/bart-preneel-4451412/
@bpreneel1 - preneel@infosec.exchange
Cedarcrypt, 13 July 2026
KU LEUVEN
COSIC

1


Cryptography Timeline
kings, generals & diplomats
wireless & commerce
finance
finance comms
Internet GSM EMV
crypto-currencies
messaging
PQC
pre-1920
1920-1960
1960-1975
1975-1990
1990-2013
2013-2025
2025
mechanical
electro-mechanical
electronics
large-scale adoption
mass adoption end-2-end
ubiquitous
software

2


I
1975-1998
stopping
research &
publications

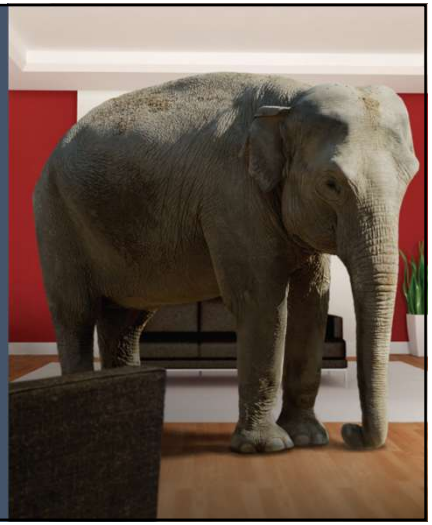
3


II
1993-1995
Clipper chip
SINK CLIPPER!
RSA

4

CALEA [1994] Communications Assistance for Law Enforcement Act

- Intercept calls or meta data with warrant
- Extended to VoIP (2004)
- EU:
  - Lawful interception:
    - Council Resolution of 17 January 1995
    - Added to 3G standards
  - Data Retention directive 2006/24/EC
    - ECJ declares it invalid for violating fundamental rights (8 April 2014)
    - EU extends data retention to over the top services (2022)



5

6

Former FBI Director James Comey

[2014] We are going dark.

We aren't seeking a back-door approach. We want to use the front door, with clarity and transparency, and with clear guidance provided by law. *We are completely comfortable with court orders and legal process.*

7

8

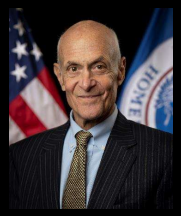
Former NSA/DHS Directors against key escrow [2015]

The US is “better served by stronger encryption, rather than baking in weaker encryption,”

“In retrospect, we mastered the problem we created by the lack of the Clipper Chip,” he said. “We were able to do a whole bunch of other things. Some of the other things were metadata, and bulk collection and so on.”

https://www.networkworld.com/article/2990294/former-nsa-chief-undercuts-fbi-s-desire-for-encryption-backdoors.html

Mike McConnell



Michael Chertoff

Michael Hayden

9

10

San Bernardino, CA, December 2, 2015

11

At the request of the FBI, based on an all writs order (1789), a U.S. federal magistrate judge has ordered Apple to break the security of the iPhone

12

The many problems of a backdoor

- Human right activists
- Journalists
- Trade secrets
- Critical infrastructure
- Autonomous vehicles
- …

13

Court case ends

March 28, 2016 FBI gets access with help of a company at the cost of US$ 900K

…yielded almost no useful information

Sept. 2016: Sergei Skorobogatov (Cambridge University) shows that access is feasible with $100 of equipment

14

$e^{i\pi} = 999$

Australian PM
Malcolm Turnbull
16 July 2017

Laws of mathematics 'do not apply' in Australia

Encryption law: 8 December 2018

15

"Warrant-proof encryption defeats the constitutional balance by elevating privacy above public safety,"

What's needed is "responsible encryption … secure encryption that allows access only with judicial authorization.

Deputy attorney general
Rod Rosenstein
9 Nov. 2017

16

The Law Enforcement argument

- The role of law enforcement is to protect society
- We have always had warrants to get access to information
- Technology should not change this

17

The Law Enforcement argument

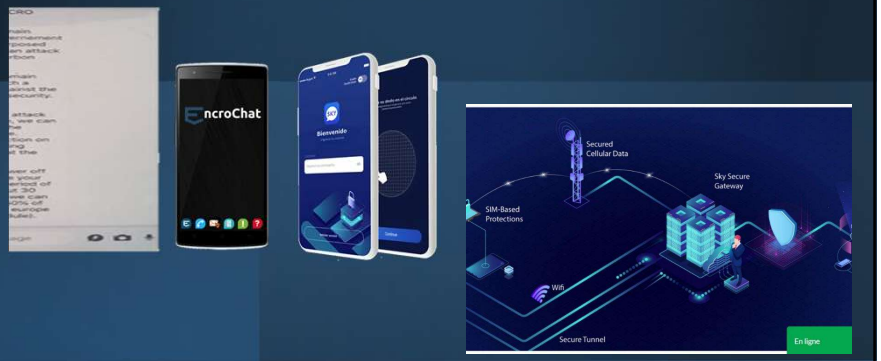
- Supporting data limited
- Washington Post, May 22, 2018 << 7800 locked phones in 2017


National Security

FBI repeatedly overstated encryption threat figures to Congress, public

18

Phantom Secure (‘18) – Anom (‘18) – Encrochat (‘20) – Sky ECC (‘21) – Exclu (‘23)



https://www.darkreading.com/endpoint/exclu-shutdown-underscores-outsized-apps-messaging-apps-role-in-cybercrime

19

Can cryptography solve the problem created by cryptography?

20

FBI Director Christopher Wray

[2018] We can find solutions to the Going Dark problem.
…
If we can develop driverless cars … surely we should be able to design devices that both provide data security and permit lawful access with a court order.

21

The civil society/academic argument [Keys under doormats 2015]

- The state of security and privacy is not good while society is becoming critically dependent on information technology
- Adding intercept capabilities will further undermine security by increasing complexity
- Risk of abuse by bad actors (e.g. non-democratic nations) and for mass surveillance
  - Examples: Greek Vodafone incident, Juniper, Calea (Salt Typhoon), Cisco
- Will not help for smart criminals and spies
- Incompatible with technologies such as perfect forward secrecy and 1-key authenticated encryption
- No solutions are known that offer reasonable tradeoffs

https://blog.xot.nl/2015/12/08/the-second-crypto-war-is-not-about-crypto/

22

Technical proposals (2017-2018)

- (Bellare-Goldwasser, Verifiable partial key escrow, 1997)
- Wright-Varia, Crypto crumble zones, Usenix Security 2018, https://www.usenix.org/node/208172
- Ray Ozzie: "Clear" – decryption key with corporations
  - Steven Levy, Cracking the Crypto War, Wired, 25 April '18
  - https://github.com/rayozzie/clear/blob/master/clear-rozzie.pdf
- Stefan Savage: Lawful device access without mass surveillance risk, ACM CCS 2018: 1761-1774
- Ernie Brickell: A Proposal for Balancing the Security Requirements from Law Enforcement, Corporations, and Individuals, May '17
- Robert Thibadeau

23

Child Sexual Abuse Material (CSAM)
#chatcontrol
2022-202?

24

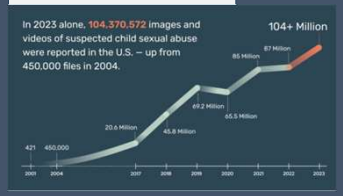
Copyright violations

- Meta removes millions of copyright-violating items annually
- Image copyright infringement is massive and structural
- Most infringements are non-malicious and unintentional
- Enforcement data runs into billions of incidents per year
- Automated detection dominates enforcement

CSAM detection
(Child Sexual Abuse Material)

NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN

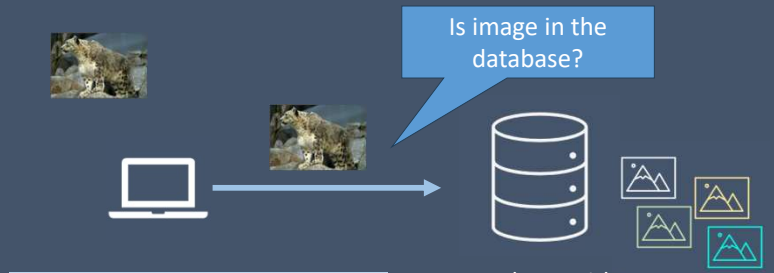
THORN



25

25

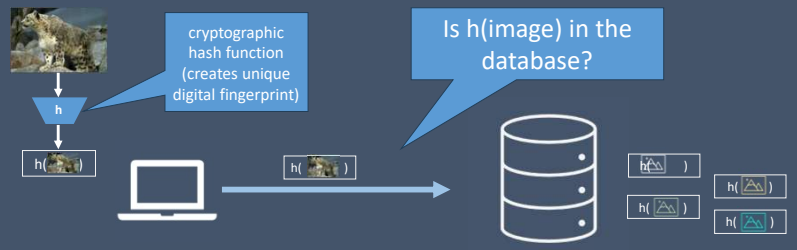
Detection of known illegal images



26

26

Detection of known illegal images (improved)



27

27

Cryptographic hashing of images

small (invisible) change to the image
⇒ completely different hash value
⇒ detection failure

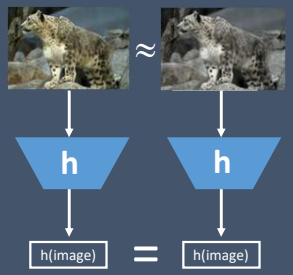
28

28

Solution: perceptual hash function

Hash function for which perceptually identical content gives the same result (or a similar result)

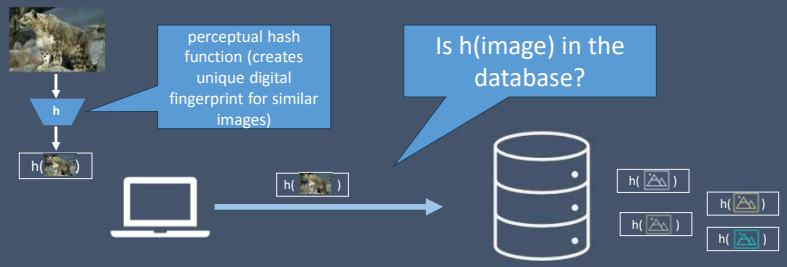
- Color consistency (e.g. brightness)
- Structural similarity (e.g. rotation)
- Content preservation (e.g. compression)
- Noise robustness



29

29

Detection of known illegal images



smaller database
privacy preserving

Database with hash values of illegal images

30

30

History of Perceptual Hash Functions

- 2007 Content ID (YouTube)
- 2009 PhotoDNA [Farid + Microsoft]
- 2010 pHash [Zauner] – open
- 2014 PhotoDNA deployed by NCMEC
- 2018 eGlyph [Farid] (YouTube)
- 2019 PDQ and TMK + PDQF (Facebook) – open
- 2021 NeuralHash (Apple) – partially open

Security by obscurity – compatible with use at service providers

31

31

Threshold private set intersection (PSI) with associated data (tPSI-AD) [July'21]

https://www.apple.com/child-safety/pdf/Apple_PSI_System_Security_Protocol_and_Analysis.pdf

- Cryptographically optimal way to detect abusive material
- Secure two-party computation (2PC)
  - server provides scanning algorithm
  - learns metadata if and only if there are multiple matches
- Cryptographically solid but…
  - Problematic: Bugs in our Pockets: the Risks of Client-Side Scanning, https://arxiv.org/abs/2110.07450, Oct. 21
  - Needs perceptual hash function: NeuralHash (96 bits)


The Apple PSI System

Abhishek Bhowmick Apple Inc. · Dan Boneh Stanford University · Steve Myers Apple Inc.

Kunal Talwar Apple Inc. · Karl Tarbe Apple Inc.

July 29, 2021

Abstract

This document describes the constraints that drove the design of the Apple *private set intersection* (PSI) protocol. Apple PSI makes use of a variant of PSI we call *private set intersection with associated data* (PSI-AD), and an extension called *threshold private set intersection* with associated data (tPSI-AD). We describe a protocol that satisfies the constraints, and analyze its security. The context and motivation for the Apple PSI system are described on the main project site.

32

32

Problem: NeuralHash collisions

collides with

Birthday paradox also works: need 2^{48} effort (2 in 2 trillion)

Apple: "These attacks are not feasible for the average user"

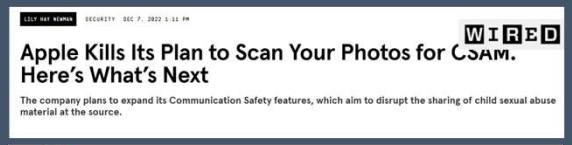
Athalye, A.: NeuralHash Collider (2021), https://github.com/anishathalye/neural-hash-collider
Kilcher, Y.: Neural Hash Collision Creator (2021), https://github.com/yk/neural_hash_collision

33

33

Update on Apple's PSI protocol

[Dec'22]



[Sep'23]

34

34

EU CSAM Regulation Proposal (May 2022)

https://eur-lex.europa.eu/resource.html?uri=cellar:13e33abf-d209-11ec-a95f-01aa75ed71a1.0001.02/DOC_1&format=PDF

- Proposal from EU Commission
- Communications shall not be scanned (ePrivacy directive) but we make an exception for CSAM
- Widespread use of end to end encryption makes scanning in servers impossible
- Hence: Mandatory **Client Side Scanning** (CSS) for known CSAM
- Scan also for new CSAM (using AI) and for grooming in chat (#CHATCONTROL)
- Age verification and assessment

35

35

EU Parliament complementary impact assessment (April '23)

https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2023)740248

1. It does not work – false positives, false negatives, bypass
2. Function creep: terrorism and organized crime
3. It will be abused by (wannabe) dictators
4. It will undermine security
5. Chilling effect on teenagers exchanging images
6. Not proportional: should be limited to private messages of persons already under suspicion of soliciting child abuse or distributing CSAM

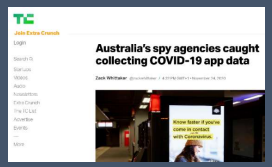
Bugs in our Pockets: the Risks of Client-Side Scanning, https://arxiv.org/abs/2110.07450 (Oct. 21)

36

36

Problem: Mission Creep

terrorist recruitment
other criminal activity

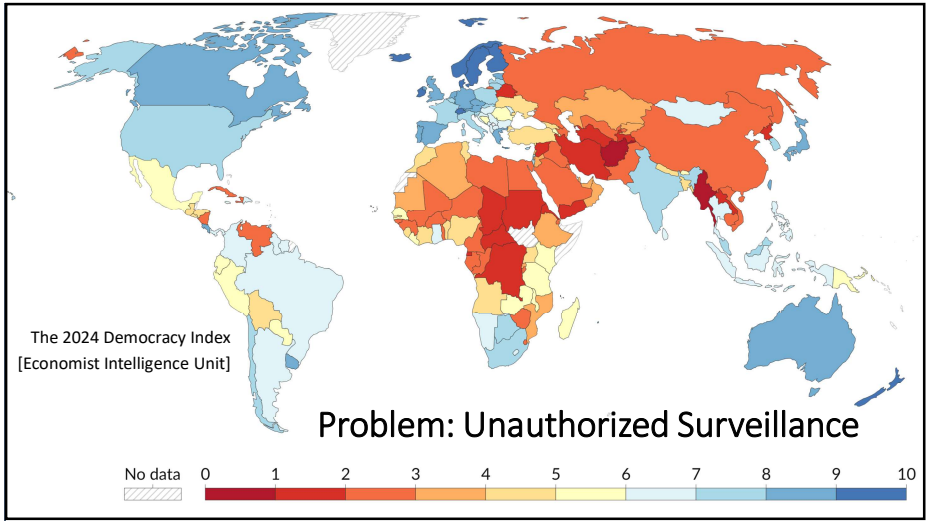


Singapore reveals Covid privacy data available to police

COVID contact tracing sheet leaves 'creepy' barman to text model

Digital Staff • 7NEWS Published: Saturday, 12 September 2020 11:03 am AEST

37



38

EU CSAM Regulation Proposal (status 2026)

https://eur-lex.europa.eu/resource.html?uri=cellar:13e33abf-d209-11ec-a95f-01aa75ed71a1.0001.02/DOC_1&format=PDF

- Parliament says no to mandatory Client Side Scanning (February '24), known as Chatcontrol 2.0
- Member states need 2 years to agree:
  - optional Client Side Scanning + obligations for high-risk services
  - new CSAM and grooming put on hold
- Chatcontrol 1.0: Parliament says no to temporary exception to scanning unencrypted communications (April '26) but after three (!) votes it was extended until 2028
- Trilogue ongoing on Chatcontrol 2.0… (2026)

https://edri.org/our-work/csa-regulation-document-pool/

39

39

NeuralHash Q&A

"Will CSAM detection in iCloud Photos falsely report innocent people to law enforcement?

No. The system is designed to be very accurate, and the likelihood that the system would incorrectly identify any given account is less than one in one trillion per year."

Disproved for malicious attacks
But what about regular users who upload selfies and photos of their kids?

40

40

Black-box attacks

- Do not assume any knowledge of the internal operation of the perceptual hash function
- Output size is known
- Can call the function on any "reasonable" image

- Here applied to NeuralHash (but also works for PhotoDNA)

41

41

False positives for CSAM detection at scale

[NCMEC, Thorn]
2022 CSAM databases contain 17.5 to 19 million images
Likely to grow based on GenAI (2026: 124 million)

In 2019 an EU citizen has taken on average 597 selfies per year
Assume that a citizen is reported only after x alerts

# alerts x before reporting	1	2	3	5	8	10
# falsely reported citizens reported in year 1	406M	304M	185M	39M	1.2M	69K

D. Leblanc-Albarel, BP: Black-box Collision Attacks on the NeuralHash Perceptual Hash Function. IACR Cryptol. ePrint Arch. 2024: 1869 (2024) (to appear in Usenix Security 2026)

42

42

White-box attacks on PhotoDNA

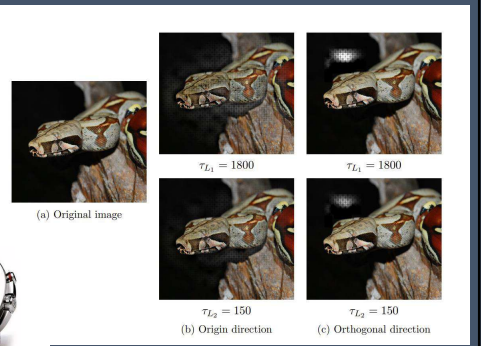
- 2021: executable leaked on GitHub
- 2022-2025: several black box attacks using ML
- 2025: our results
  - identified the complete description "Alleged PhotoDNA" (verified on 50K examples)
  - substantial improvement of all attacks: faster, closer distance, less noisy
    - thresholds: τ_{L1} = 1800 and τ_{L2} = 150-200

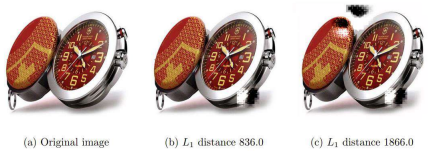
43

43

Detection avoidance (false negative) (1/2)

- Global vs. localized changes
- 100% vs. 96.4% success rate
  - 2nd run with different orthogonal vector
- Mean time: 9.94 vs. 78.48 s





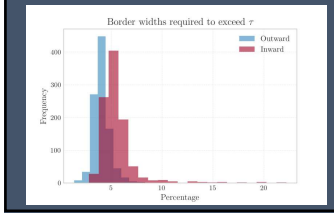
44

Slide credit: Maxime Deryck

44

Detection avoidance (false negative) (2/2)

Outward 5% (reversible)



Inward

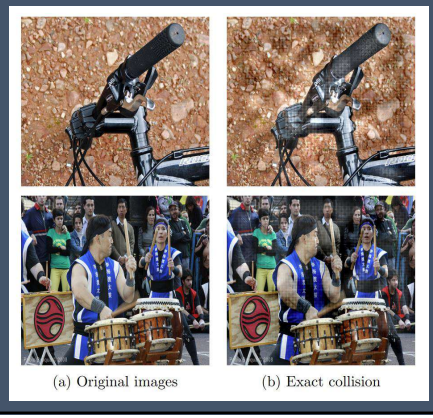
45

Slide credit: Maxime Deryck

45

Collision attack

- Gradient descent on composite loss with focus on hash collision
- 100% success rate
- Fast convergence (mean: 4159 iterations)
- Mean time: 215.14 s (97.29 - 420.69 s)
- Can be improved



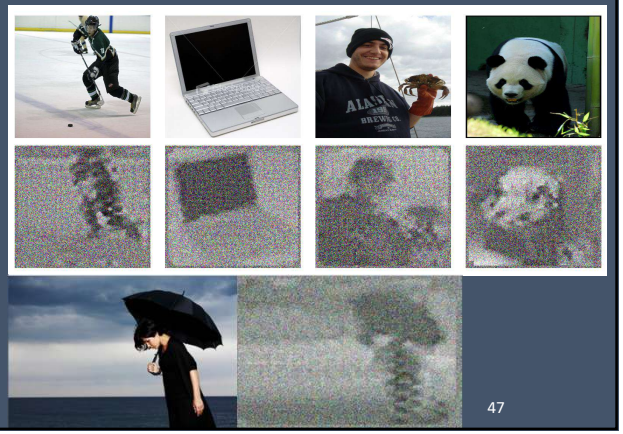
(a) Original images (b) Exact collision

Slide credit: Maxime Deryck

46

Preimage attack: information leakage

- Gradient descent on L1 (hash) loss
- Sensitive to starting image: restarts needed
- 99.5% success rate
  - remaining 5 images succeeded after manually adjusting learning rate
  - 88.0% success after first (re)start
- Mean time: 11.2 s for one restart (max. 2357 iterations)



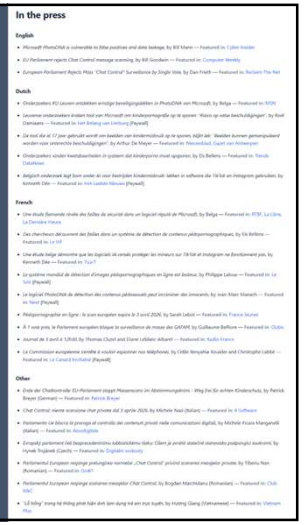
Slide credit: Maxime Deryck

47

47

Status: https://pseudodna.eu/

- PhotoDNA does not achieve its design goals:
  - 1 in 50 billion false positives
  - 1% false negatives
  - irreversibility
- M. Deryck, D. Leblanc-Albarel, B. Preneel, White-Box Attacks on PhotoDNA Perceptual Hash Function, IACR eprint 2026/486



48

Coordinated vulnerability disclosure to Microsoft
[October 2025]

"After a thorough evaluation, our engineering teams have determined that the behavior described does not constitute a security vulnerability and therefore does not meet Microsoft's criteria for immediate intervention. The issues described in this research correspond to the known limitations of this type of technology (perceptual image hashing), including PhotoDNA. These systems are not intended to provide cryptographic security guarantees, and malicious manipulation of perceptual hashes is a widely recognized limitation in this field."

https://www.microsoft.com/en-us/photodna (26 April 2026):

- "A PhotoDNA hash is not reversible, and therefore cannot be used to recreate an image."

49

49

Are there other options for law enforcement to deal with encryption?

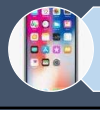
50

Which access is needed?

Communications: voice
- telephony: phone or cell tower
- VOIP

Communications: data
- messages
- meta data

Stored data
- cloud
- media (USB)



Devices
- confiscated
- remote

51

Options for Law Enforcement

- **exploit operational security weaknesses:** operating a system securely is difficult
  - e.g. password cracking
- obtain **technical assistance from industry** to bypass decryption or to access keys
  - remote update
  - backup in cloud
  - iPhone unlock from Cellebrite or Grayshift
- **use metadata**
- **use AI**

52

Apple vs. the UK

Apple starts rolling out end-to-end cloud encryption

Apple "can no longer offer Advanced Data Protection" in

2022 | 7 Feb. 2025 | 21 Feb. 2025 | 8 Apr. 2025

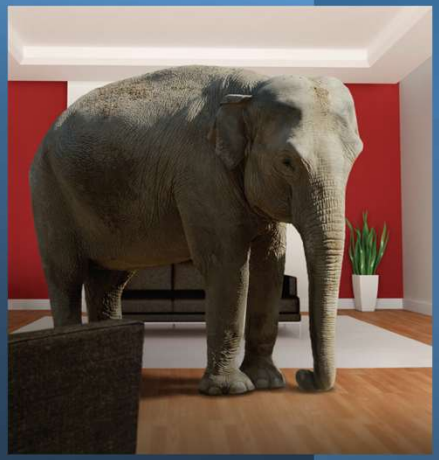
The UK government demands ability to access encrypted data stored by Apple users worldwide in its cloud service based on the 2016 Investigatory Powers Act

Apple is suing UK government over encryption backdoor request

53

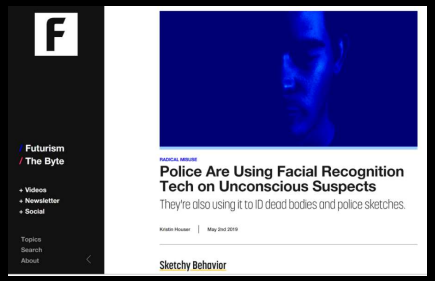
metadata

Law enforcement: metadata is insufficient



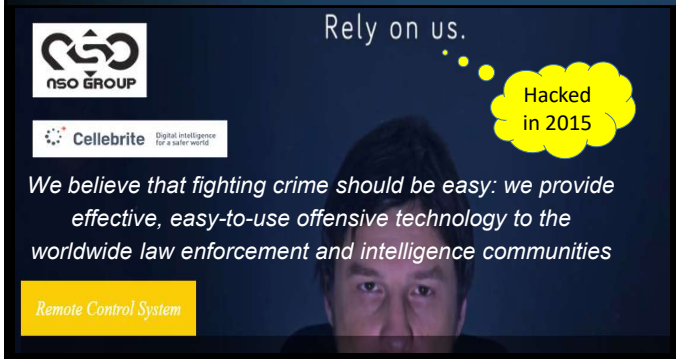
54

AI?



55

Options for Law Enforcement: hacking

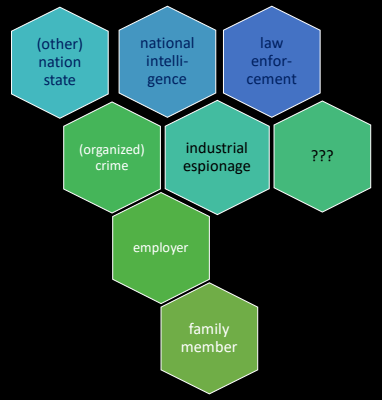


exploit known and unknown vulnerabilities (0-days) to get access

DE: Bundestrojaner: key logger, screenshots, Skype calls

56

The bigger picture



57

But who shall watch over the (cyber) guards?

58

The fifth Crypto War is coming

59

ProtectEU Internal Security Strategy

(April 1, 2025)
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025PC0148

The Commission will:

- present a Roadmap setting out the way forward on lawful and effective access to data for law enforcement in 2025
- prepare an impact assessment in 2025 with a view to updating rules on data retention at EU level, as appropriate
- present a Technology Roadmap on encryption to identify and assess technological solutions to enable lawful access to data by law enforcement authorities in 2026

60

Age verification

- Effectiveness not proven by scientific studies
- Undermines the architecture of the open internet
- Easy to circumvent: adult's smartphone, VPN, hack
  - may lead to blocking of websites and ban of VPNs
- Chilling effect on all users
- Exclusion for socially weak

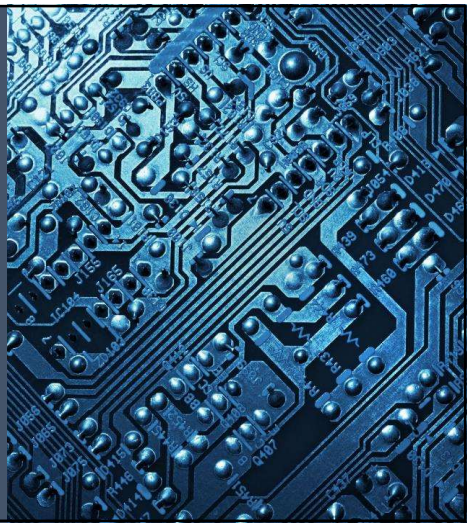
- ZK gives privacy but does not avoid all the problems
- And yes, age assessment is worse

61

61

Conclusions

- Technology is fundamentally changing power relationships
- Increased power by big tech, law enforcement, intelligence services, military
- Cryptography can help to bring some balance
- Crypto wars will continue
- Upcoming: EU Digital Wallet



62

Bart Preneel

ADDRESS: Kasteelpark Arenberg 10, 3000 Leuven
WEBSITE: homes.esat.kuleuven.be/~preneel/
EMAIL: Bart.Preneel@esat.kuleuven.be
MASTODON: bpreneel@infosec.exchange
TWITTER: @bpreneel1
TELEPHONE: +32 16 321148

KU LEUVEN COSIC

63

63

Some Links: crypto wars

1996: Cryptography's Role in Securing the Information Society
1997: The risks of key recovery, key escrow, and trusted third-party encryption. World Wide Web J. 2: 241-257
2015: Keys under doormats: https://dl.acm.org/doi/10.1145/2814825
2017: Susan Landau, Listening in, Cybersecurity in an Insecure Age
2018: Decrypting the Encryption Debate. A Framework for Decision Makers
2019: Jim Baker, Susan Landau: https://www.lawfaremedia.org/article/new-perspectives-future-encryption
2023: Cryptography and the Intelligence Community: The Future of Encryption, https://nap.nationalacademies.org/resource/26168/Highlights_for_Cryptography_and_the_Intelligence_Community.pdf
https://edri.org/tag/going-dark/

https://en.wikipedia.org/wiki/Greek_wiretapping_case_2004%E2%80%9305
https://blog.cryptographyengineering.com/2015/12/22/on-juniper-backdoor/
https://www.cs.utexas.edu/~hovav/dist/juniper.pdf
https://urgentcomm.com/cybersecurity/calea-vulnerability-exploited-in-salt-typhoon-attack-on-carriers-speaker-tells-congress

64

Some Links: CSAM

EDRI's overview: https://edri.org/policy-files/csa-regulation

Susan Landau: https://www.lawfaremedia.org/article/the-shapeshifting-crypto-wars

CSAM Open letters by academics:

- July'23: https://docs.google.com/document/d/13Aeex72MtFBjKhExRTooVMWN9TC-pbH-5LEaAbMF91Y
- May'24: https://nce.mpi-sp.org/index.php/s/eqjiKaAw9yYQF87
- Aug'24: https://homes.esat.kuleuven.be/~preneel/Open_letter_CSAR_aug24_still_unacceptable.pdf
- Sep'25: https://csa-scientist-open-letter.org/Sep2025
- Nov'25: https://csa-scientist-open-letter.org/Nov2025

https://mullvad.net/en/why-privacy-matters/going-dark

Petition by Global Encryption Coalition (May'24): https://actionnetwork.org/petitions/global-encryption-coalition-joint-statement-on-the-dangers-of-the-may-2024-council-of-the-eu-compromise-proposal-on-eu-csam/thankyou

Statement by Signal (Jun'24): https://signal.org/blog/pdfs/upload-moderation.pdf

Bugs in our Pockets: the Risks of Client-Side Scanning, https://arxiv.org/abs/2110.07450

65

Some links: Perceptual hash functions

Apple NeuralHash: https://blog.roboflow.com/neuralhash-collision/
Microsoft PhotoDNA: https://hackerfactor.com/blog/index.php?/archives/931-PhotoDNA-and-Limitations.html

Meta: TMK + https://www.hackerfactor.com/blog/index.php?/archives/971-FB-TMK-PDQ-WTF.html

Struppek, L., Hintersdorf, D., Neider, D., Kersting, K.: Learning to Break Deep Perceptual Hashing: The Use Case NeuralHash. In: Proc. 2022 ACM Conference on Fairness, Accountability, and Transparency. pp. 58–69

J. Prokos, N. Fendley, M. Green, R. Schuster, E. Tromer, T.M. Jois, Y. Cao: Squint Hard Enough: Attacking Perceptual Hashing with Adversarial Machine Learning. USENIX Security Symposium 2023: 211-228 https://www.usenix.org/conference/usenixsecurity23/presentation/prokos

D. Leblanc-Albarel, B. Preneel, Black-box Collision Attacks on the NeuralHash Perceptual Hash Function. IACR Cryptol. ePrint Arch. 2024: 1869 (2024) (to appear in Usenix Security 2026)

M. Deryck, D. Leblanc-Albarel, B. Preneel, White-Box Attacks on PhotoDNA Perceptual Hash Function, IACR eprint Cryptol. ePrint Arch. 2026/48

66

66

Some Links: research

James Bartusek, Sanjam Garg, Abhishek Jain, Guru-Vamsi Policharla, End to End Secure Messaging with Traceability Only for Illegal Content, Eurocrypt 2023

Pedro Branco, Matthew Green, Aditya Hegde, Abhishek Jain, and Gabriel Kaptchuk, How to Trace Viral Content in End-to-End Encrypted Messaging, https://eprint.iacr.org/2025/1052.pdf

Scott Griffy, Markulf Kohlweiss, Anna Lysyanskaya, Meghna Sengupta, Succinctly Verifiable Computation over Additively-Homomorphically Encrypted Data: Making Privacy-Preserving Blueprints Practical, https://eprint.iacr.org/2024/675

67