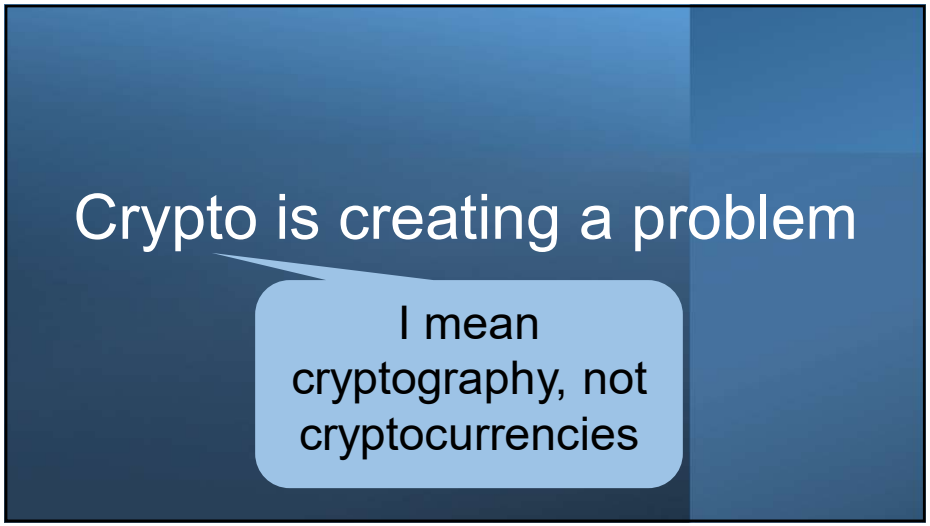
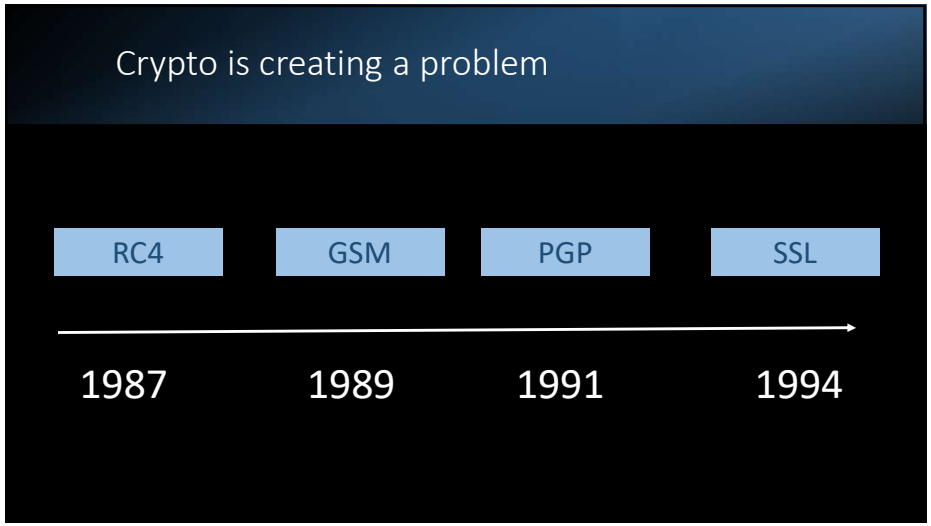

The ongoing crypto wars
Bart Preneel
firstname.lastname@esat.kuleuven.be
@bpreneel1 - preneel@infosec.exchange
SecAppdev, 2 June 2026
KU LEUVEN
COSIC
ArenBerg Crypto BV

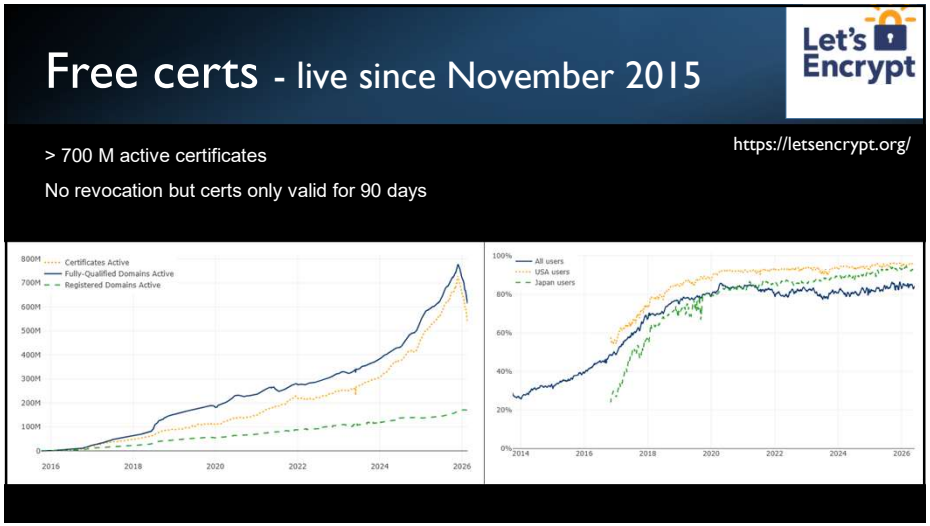
1


Crypto is creating a problem
I mean cryptography, not cryptocurrencies

2


Crypto is creating a problem
RC4
GSM
PGP
SSL
1987
1989
1991
1994

3


Free certs - live since November 2015
Let's Encrypt
> 700 M active certificates
https://letsencrypt.org/
No revocation but certs only valid for 90 days

4

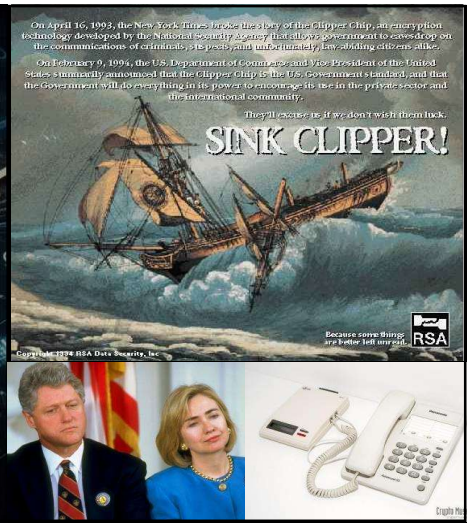
I

1975-1998
stopping
research &
publications

5

II

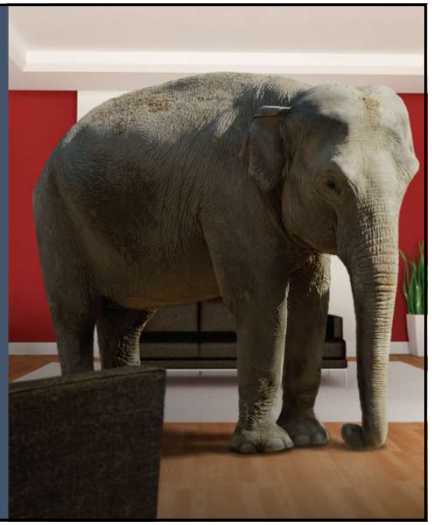
1993-1995
Clipper chip



6

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)



7

III

2015-2018

8

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.*

9

"[I]n our country, do we want to allow a means of communication between people which we cannot read?" [Jan 2015]

UK: Investigatory Power Act 2016 [Snooper's Charter]

10

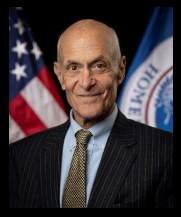
Former NSA/DHS Directors against key escrow [2015]

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

11

12

San Bernardino, CA, December 2, 2015

13

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

14

The many problems of a backdoor

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

15

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

16

$e^{i\pi} = 999$

Australian PM
Malcolm Turnbull
16 July 2017

Laws of mathematics 'do not apply' in Australia
Encryption law: 8 December 2018

17

"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

18

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

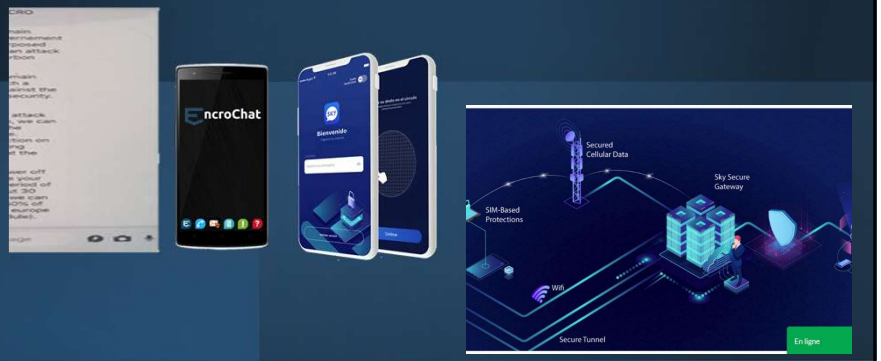
19

The Law Enforcement argument

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

20

Encrochat (‘20) – Sky ECC (‘21) – Exclu (‘23)



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

21

Can cryptography solve the problem created by cryptography?

22

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.

23

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)
- Incompatible with technologies such as perfect forward secrecy and 1-key authenticated encryption
- Will not help for smart criminals and spies
- No solutions are known that offer reasonable tradeoffs

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

24

25

Attorney General William Bar

Department of Justice
Office of Public Affairs

FOR IMMEDIATE RELEASE

Sunday, October 11, 2020

International Statement: End-To-End Encryption and Public Safety

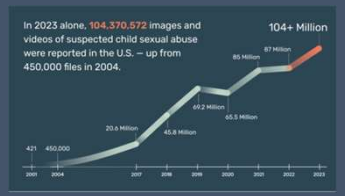
- We, the undersigned, support strong encryption, which plays a crucial role in protecting personal data, privacy […]
- Particular implementations of encryption technology, however, pose significant challenges to public safety, including to highly vulnerable members of our societies like sexually exploited children. [..]
  - Embed the safety of the public in system designs, thereby enabling companies to act against illegal content and activity effectively with no reduction to safety, and facilitating the investigation and prosecution of offences and safeguarding the vulnerable;
  - Enable law enforcement access to content in a readable and usable format where an authorisation is lawfully issued, is necessary and proportionate […]

26

The CSAM story
(Child Sexual Abuse Material

NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN

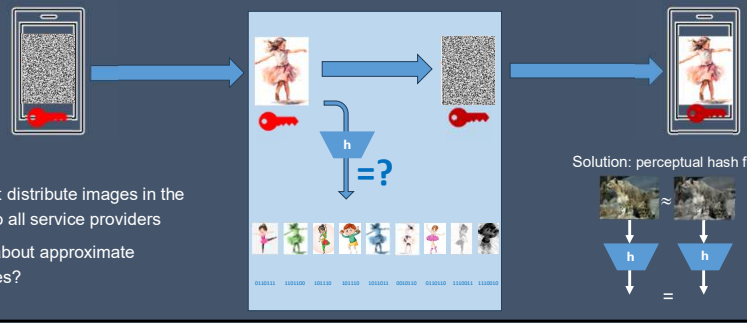
THORN



27

Known CSAM detection in server

Current database: 131+M (https://safer.io/solutions/



Cannot distribute images in the clear to all service providers

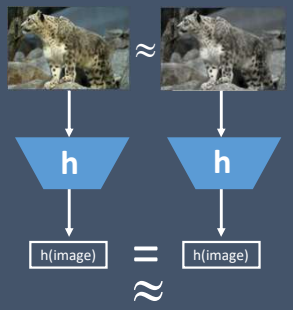
What about approximate matches?

28

Perceptual hash function

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

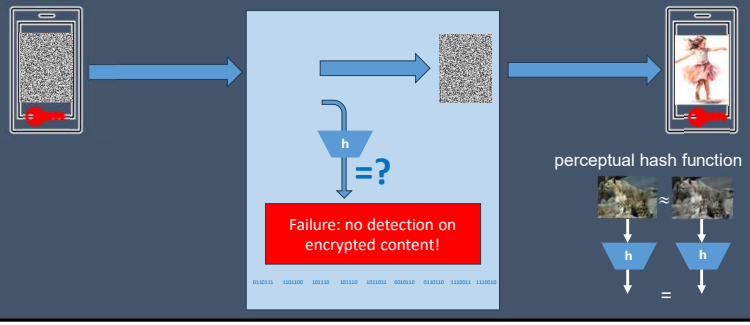
- Color consistency (e.g. brightness)
- Structural similarity (e.g. rotation)
- Content preservation (e.g. compression)
- Noise robustness



29

CSAM with end to end encryption?

Solution: client side scanning



30

EU CSAM Regulation Proposal

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472

EU Commission impact assessment (May'22)
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0209&from=EN

Dealing with end-to-end encryption

On device
1. full detection on device (client side scanning)
2. **full hashing with matching at server**
3. **partial hashing with matching at server**
4. use of classifiers

In server
5. **secure enclaves (e.g. SGX)**
6. 3rd party matching
7. MPC variant of 3rd party matching
8. on-device homomorphic encryption with server-side hashing and matching

EU Parliament complementary impact assessment (April '23)
https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2023)740248

31

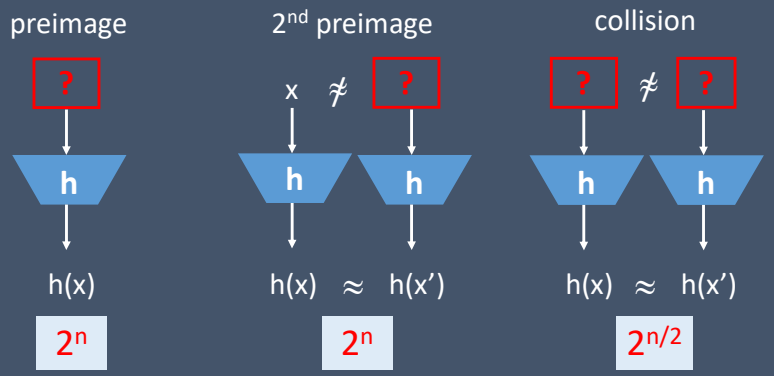
History of Perceptual Hash Functions

- 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 (does not work for client side scanning)

32

Perceptual hashing: security (n-bit result)



33

Weaknesses in perceptual hash functions

- False negatives: detection avoidance
- False positive (collisions): innocent user is flagged and surveilled
- 2nd preimage
  - surveillance: if one can induce a user to send a 2nd preimage to a hash value in a database, this user will be investigated
  - framing/censorship: adversary can add image to database that has a hash value close to that of an image a user is likely to send
- Preimage (for hash value of a user or in the database)
  - find out attribute of an image or a noisy version of the image from a hash value

Based on J. Prokos et al.: Squint Hard Enough: Attacking Perceptual Hashing with Adversarial Machine Learning. USENIX Security Symposium 2023: 211-228

34

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
Serious problems for regular users who upload selfies and photos of their kids?

35

False positives for NeuralHash (carefully crafted)

Birthday paradox also works: need 2^{48} images

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

36

False Positives for NeuralHash (accidental)

	Non-human	Non-BF	Light BF
# illegitimate collisions	0	24	25
#hash operations until collision	–	$2^{16.1}$	$2^{15.2}$

(a) Non BF (b) Light BF

37

False Positives for NeuralHash (accidental)

[NCMEC]
Current CSAM databases contain 17.5 to 19 million images
Likely to grow based on GenAI

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

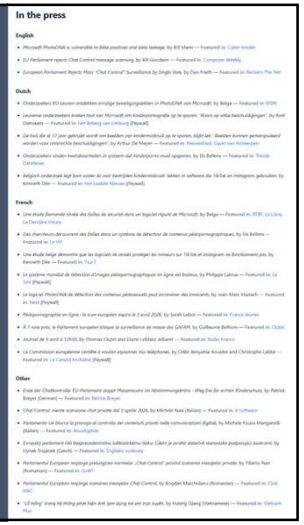
Diane Leblanc-Albarel, Bart Preneel: Black-box Collision Attacks on the NeuralHash Perceptual Hash Function. IACR Cryptol. ePrint Arch. 2024: 1869 (2024)

38

Microsoft PhotoDNA

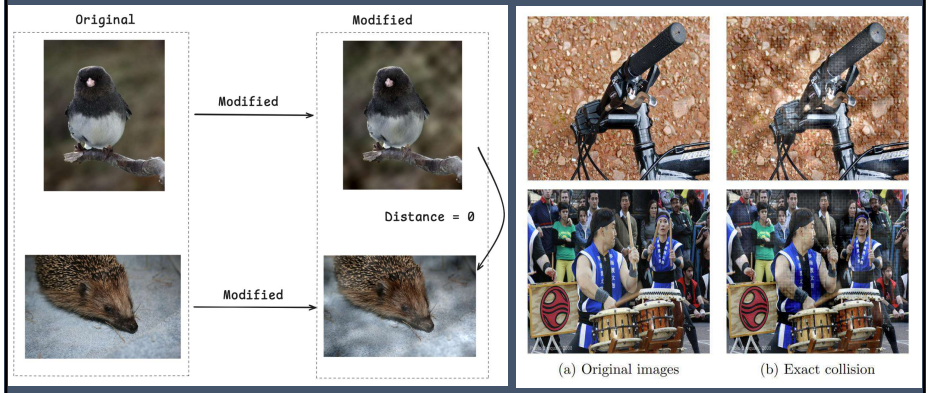
- PhotoDNA does not achieve its design goals:
  - 1 in 50 billion false positives
  - 1% false negatives
  - irreversibility
- Details: https://pseudodna.eu/

M. Deryck, D. Leblanc-Albarel, B. Preneel, White-Box Attacks on PhotoDNA Perceptual Hash Function, IACR eprint 2026/486



39

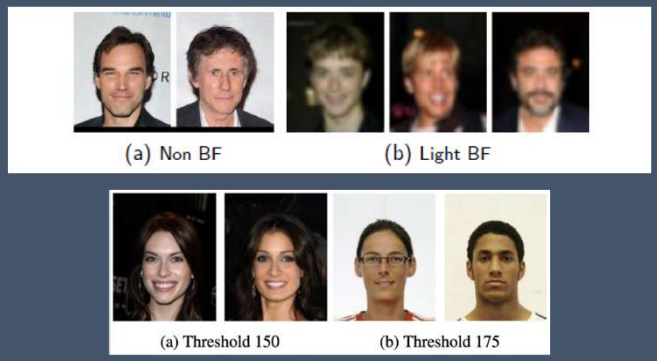
False Positives: PDQ and PhotoDNA (carefully crafted)



(a) Original images (b) Exact collision

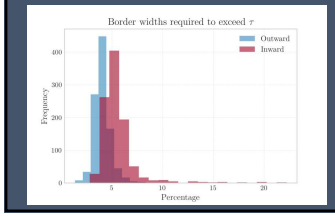
40

False positives for NeuralHash and PhotoDNA (accidental)



41

False Negative: PhotoDNA



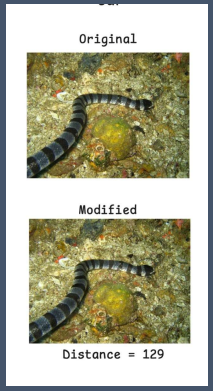
Outward 5% (reversible)

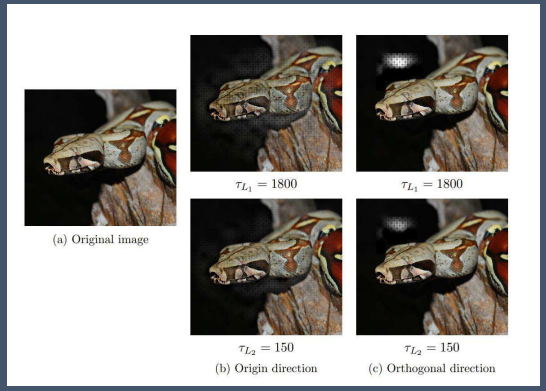
Inward

Slide credit: Maxime Deryck

42

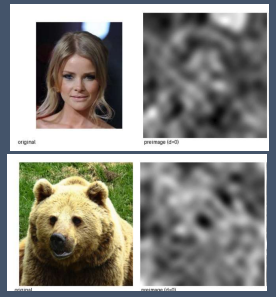
False negatives: PDQ and PhotoDNA





43

Inverting PDQ and PhotoDNA



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."

44

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."

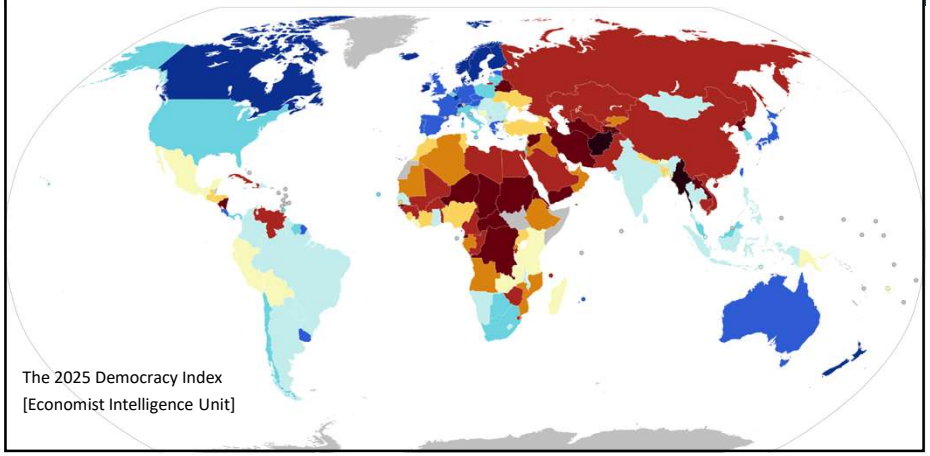
45

Problem: Detecting new content and correctly detecting grooming in written and spoken language is likely well beyond the state of the art

Thorn non-profit claims 10% false positive rate for detection of new CSAM

46

Problem: Unauthorized Surveillance

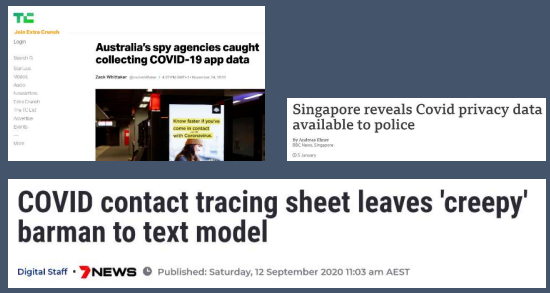


The 2025 Democracy Index
[Economist Intelligence Unit]

47

Problem:
Mission Creep

terrorist recruitment
other criminal activity



48

EU CSAM Regulation Proposal

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472roposal

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

EU Parliament votes no (Feb. '24)

2024-2025 proposals
- narrower scope
- initially voluntary
- age verification and assessment

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

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

49

Age verification

- Effectiveness not proven by scientific studies
- Undermines the architecture of the open internet
- Easy to circumvent using an adult's smartphone or a VPN
- Age requirements and rules vary by country
- Access to useful information is blocked (public education, LGBTQ+)
- Risk of exposure to even less regulated information
- Chilling effect and exclusionary effect regarding public participation
- Overfiltering and self-censorship
- Shift of liability from platforms to individuals
- Not proportional

50

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

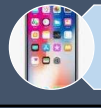
51

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

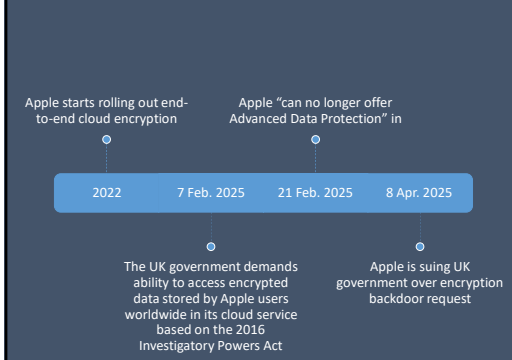
52

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**

53

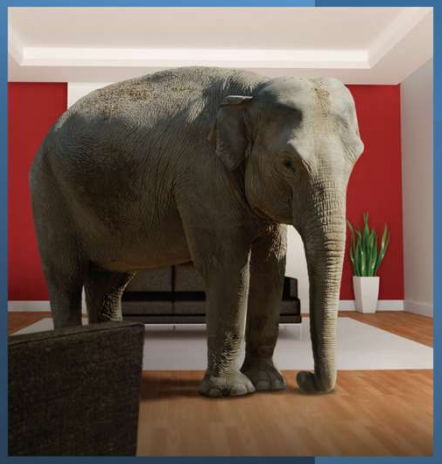
Apple vs. the UK



54

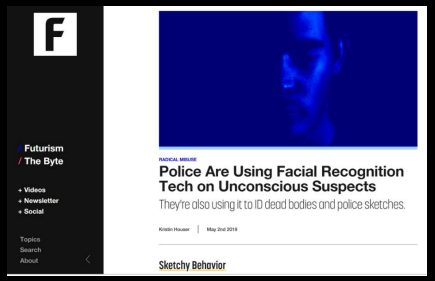
metadata

Law enforcement: metadata is insufficient



55

AI?



56


Predator
Options for Law Enforcement: hacking
Rely on us.
Hacked in 2015
NSO GROUP
Cellebrite
We believe that fighting crime should be easy: we provide effective, easy-to-use offensive technology to the worldwide law enforcement and intelligence communities
Remote Control System
exploit known and unknown vulnerabilities (0-days) to get access
DE: Bundestrojaner: key logger, screenshots, Skype calls

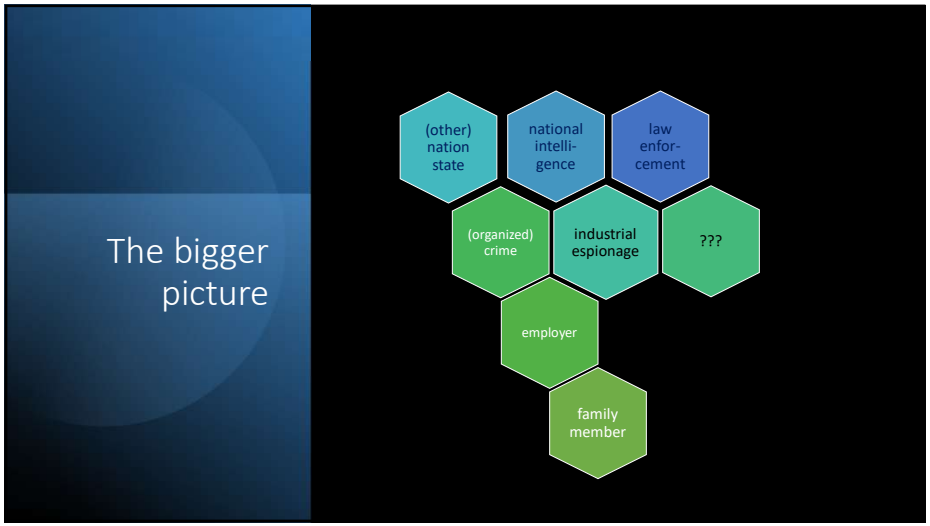
57


Options for Law Enforcement
NSA:
"Collect it all, know it all, exploit it all"
Collaborate with intelligence services

58


Response of the NSA after 1994
• Going after keys: hacks, replacing public keys, security letters (300K 2001-2016)
• Weak implementations
• Undermine standards (DUAL_EC_DRBG)
• Cryptanalysis
• Increase complexity of standards
• Export controls
• Hardware backdoors

59


The bigger picture
(other) nation state
national intelli-gence
law enfor-cement
(organized) crime
industrial espionage
???
employer
family member

60

But who shall watch over the (cyber) guards?

61

The fifth Crypto War is coming

62

ProtectEU Internal Security Strategy

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

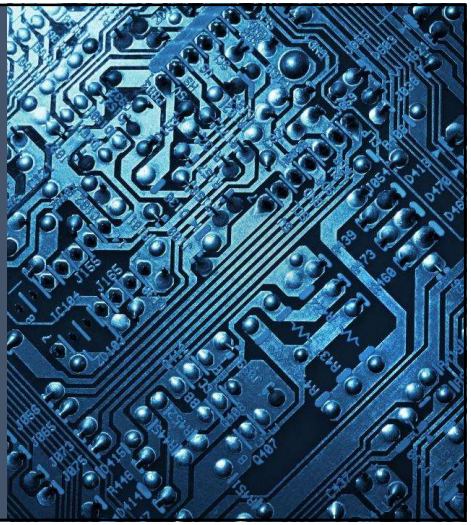
The Commission will:

- 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

63

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: Age verification and the EU Digital Wallet

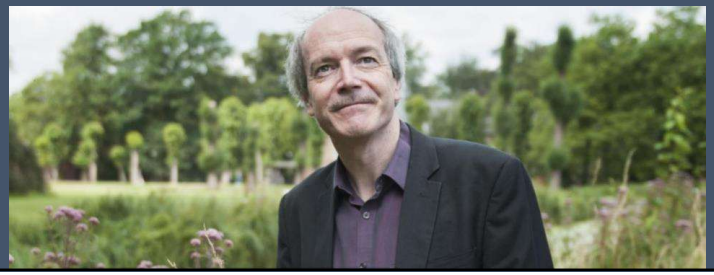


64

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
ArenBerg Crypto BV
COSIC



65

65

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

66

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
- Sept '25 /https://csa-scientist-open-letter.org/Sep2025

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
Latest CSAM proposal by Belgian presidency:
https://netzpolitik.org/wp-upload/2024/05/2024-05-28_Council_Presidency_LEWP_CSAR_Compromise-texts_9093.pdf

67

Some Links: research

Bellare-Goldwasser, Verifiable partial key escrow, 1997

Wright-Varia, Crypto crumble zones, Usenix Security 2018, https://www.usenix.org/node/208172

Stefan Savage: Lawful device access without mass surveillance risk, ACM CCS 2018: 1761-1774

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

68