KU LEUVEN

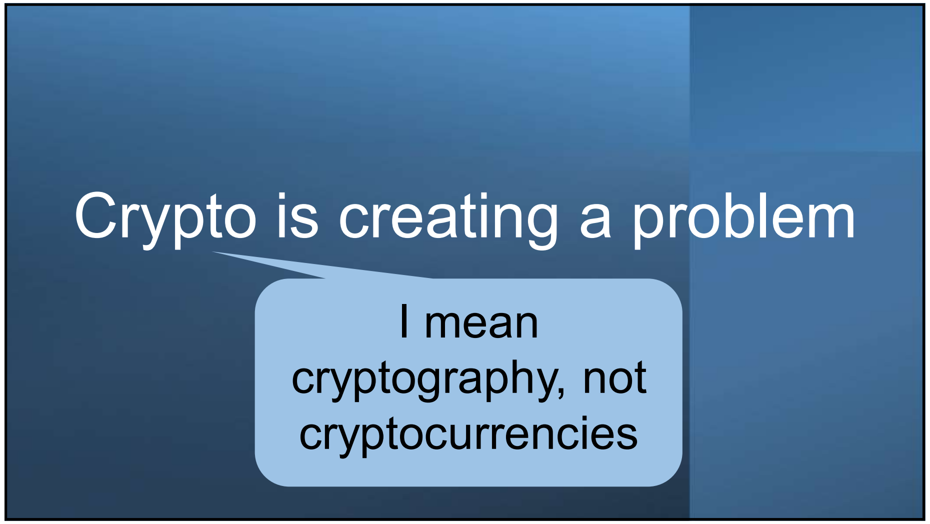
M3AAWG ENGAGEMENT SERIES

EU CSAR
aka Chat Control 2.0:
M3AAWG's position?
Bart Preneel

September 10, 2024

Confidential to M³AAWG Members

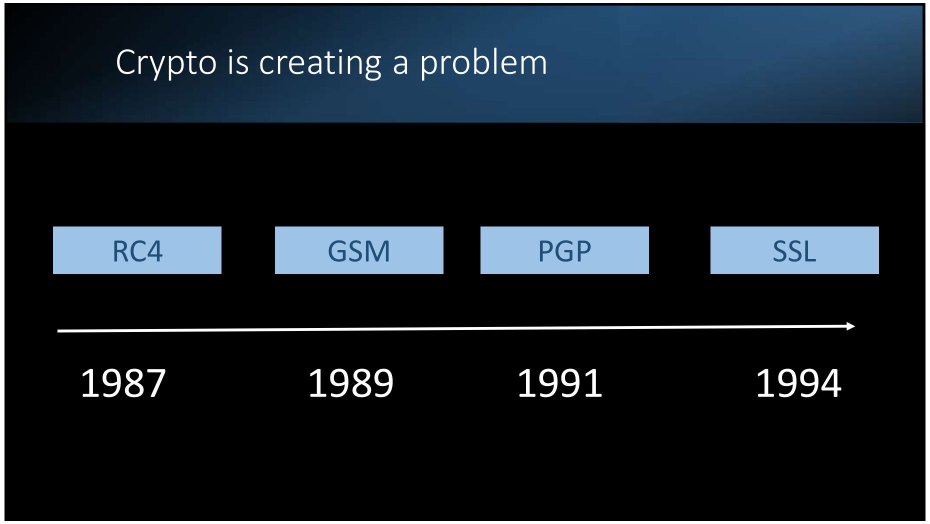
1



Crypto is creating a problem

I mean cryptography, not cryptocurrencies

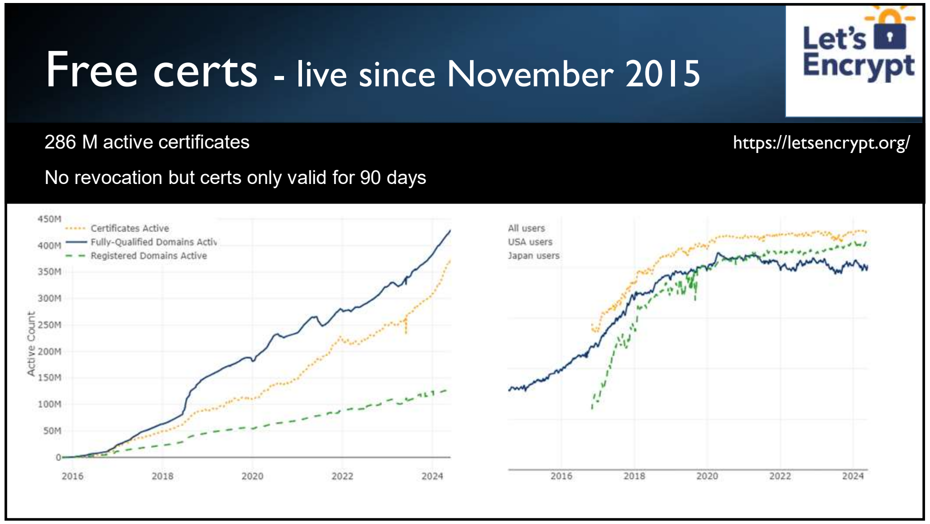
2



Crypto is creating a problem

RC4 — 1987
GSM — 1989
PGP — 1991
SSL — 1994

3



Free certs - live since November 2015

Let's Encrypt

286 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

On April 16, 1993, the New York Times broke the story of the Clipper Chip, an encryption technology developed by the National Security Agency that allows government to eavesdrop on the communications of criminals, suspects, and unfortunately, law-abiding citizens alike.

On February 9, 1994, the U.S. Department of Commerce and Vice President of the United States summarily announced that the Clipper Chip is the U.S. Government standard, and that the Government will do everything in its power to encourage its use in the private sector and the international community.

They'll excuse us if we don't wish them luck.

SINK CLIPPER!

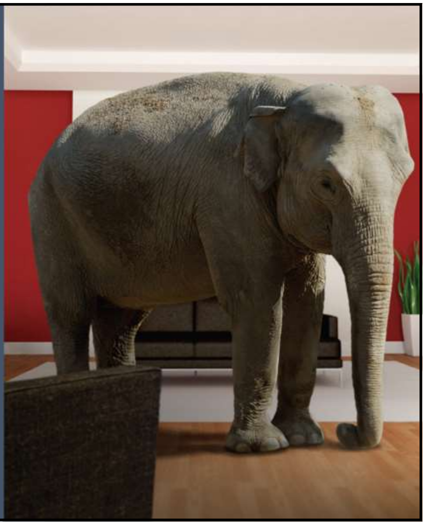
Because some things are better left unread. RSA

Copyright 1994 RSA Data Security, Inc

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)

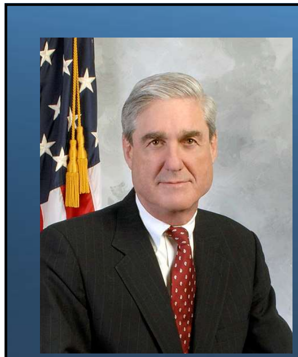


7

III

2015-2018

8



Former FBI Director
Robert Mueller

[2013] Growing gap between law enforcement’s legal authority to conduct electronic surveillance, and its ability to conduct such surveillance

9

Former FBI Director
James Comey

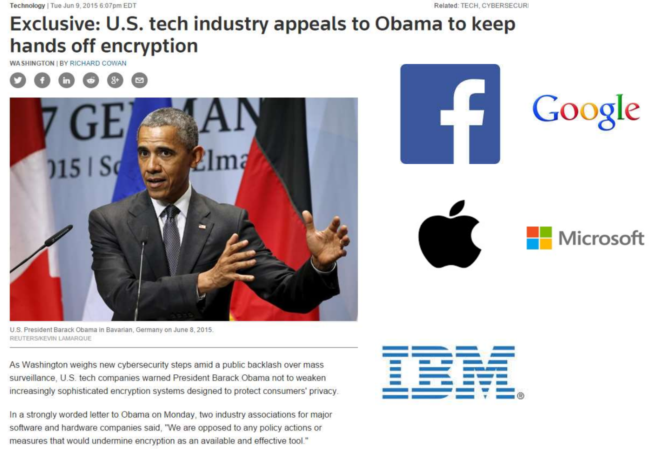
[2014] We are going dark.

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.*

10

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

11



Technology | Tue Jun 9, 2015 6:07pm EDT

Related: TECH, CYBERSECURI

Exclusive: U.S. tech industry appeals to Obama to keep hands off encryption

WASHINGTON | BY RICHARD COWAN

U.S. President Barack Obama in Bavarian, Germany on June 8, 2015.
REUTERS/KEVIN LAMARQUE

As Washington weighs new cybersecurity steps amid a public backlash over mass surveillance, U.S. tech companies warned President Barack Obama not to weaken increasingly sophisticated encryption systems designed to protect consumers' privacy.

In a strongly worded letter to Obama on Monday, two industry associations for major software and hardware companies said, "We are opposed to any policy actions or measures that would undermine encryption as an available and effective tool."

12

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

13

14

San Bernardino, CA, December 2, 2015

15

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

We JUST NeeDeD THIS ONe...
PRIVACY
FBI

16

The many problems of a backdoor

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

PANDORA'S iPHONE
BACK DOOR
FBI
HACKERS
REPRESSIVE REGIMES
ETC.

17

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

18

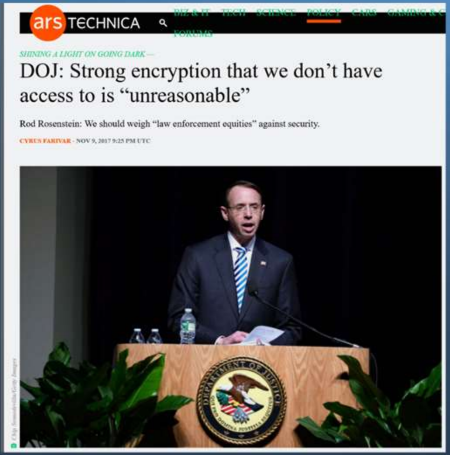
$e^{i\pi} = 999$

Australian PM
Malcolm Turnbull
16 July 2017

Laws of mathematics 'do not apply' in Australia

Encryption law: 8 December 2018

19



SHINING A LIGHT ON GOING DARK —

DOJ: Strong encryption that we don't have access to is "unreasonable"

Rod Rosenstein: We should weigh "law enforcement equities" against security.

CYRUS FARIVAR - NOV 9, 2017 9:25 PM UTC

"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

20

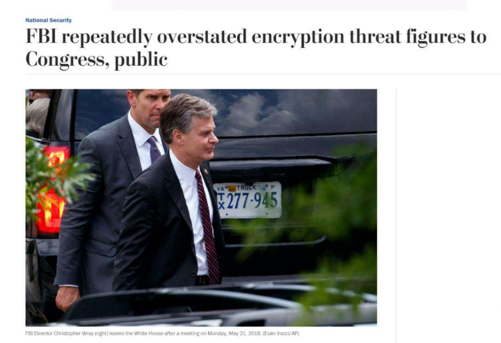
The Law Enforcement argument

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

21

The Law Enforcement argument

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



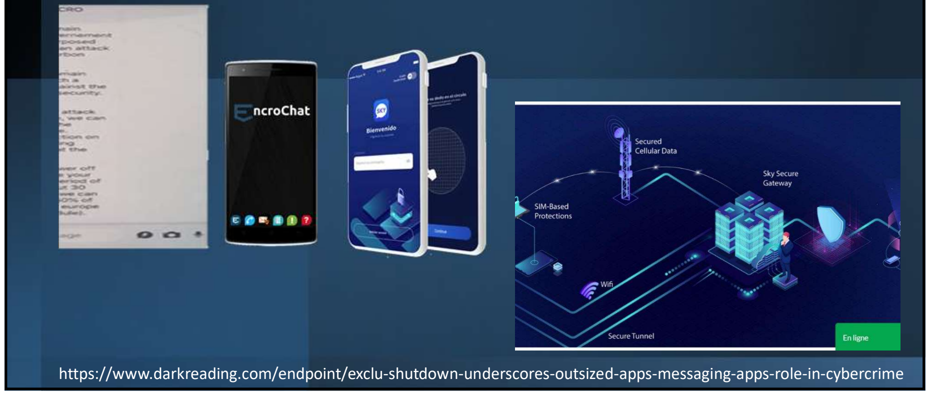
National Security

FBI repeatedly overstated encryption threat figures to Congress, public

FBI Director Christopher Wray (right) leaves the White House after a meeting on Monday, May 21, 2018. (Evan Vucci/AP)

22

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



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

23

Can cryptography solve the problem created by cryptography?

24

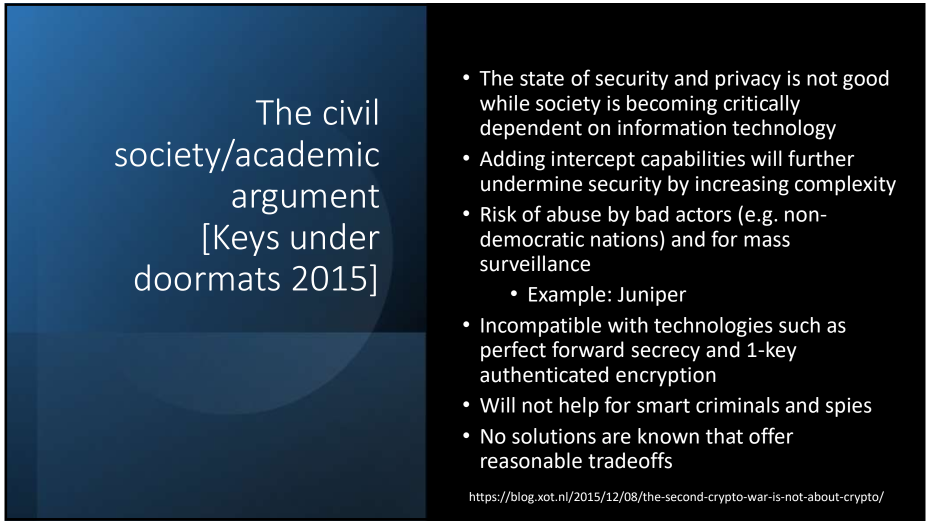
FBI Director Christopher Wray

[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.

25

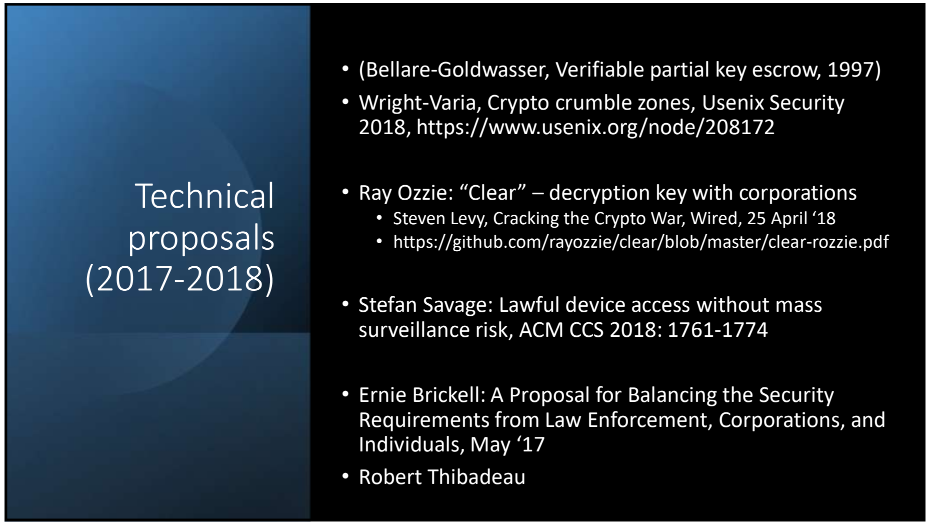


The civil society/academic argument [Keys under doormats 2015]

- 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
  - Example: Juniper
- 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/

26



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

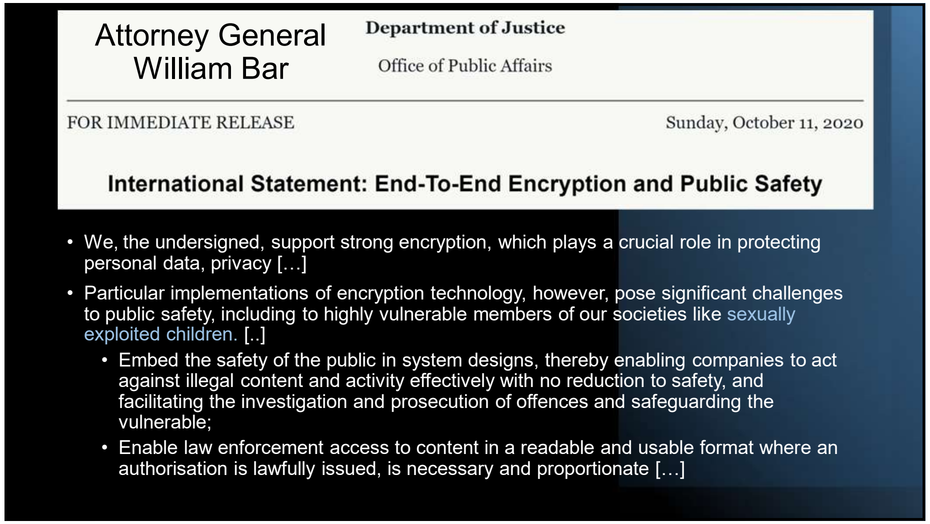
27

Child Sexual Abuse Material (CSAM)

#chatcontrol

2022-202?

28



Attorney General
William Bar

Department of Justice

Office of Public Affairs

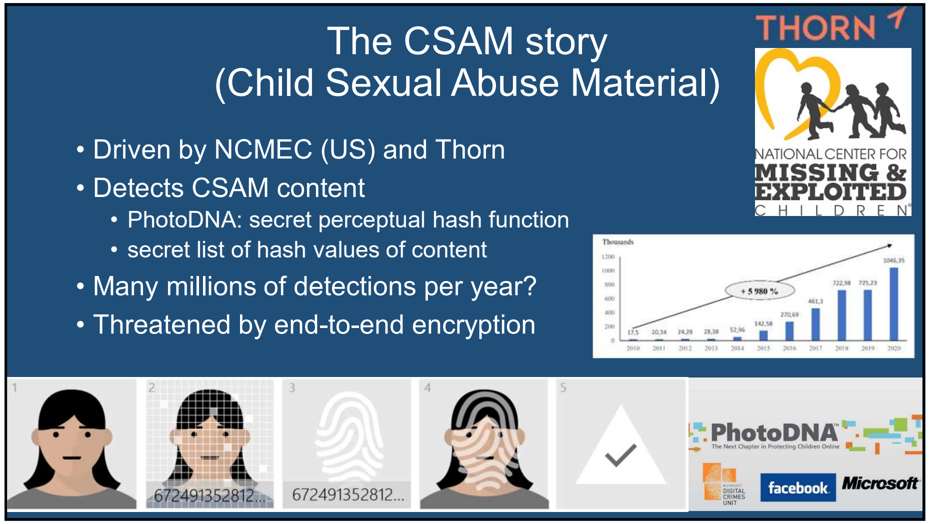
FOR IMMEDIATE RELEASE

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 […]

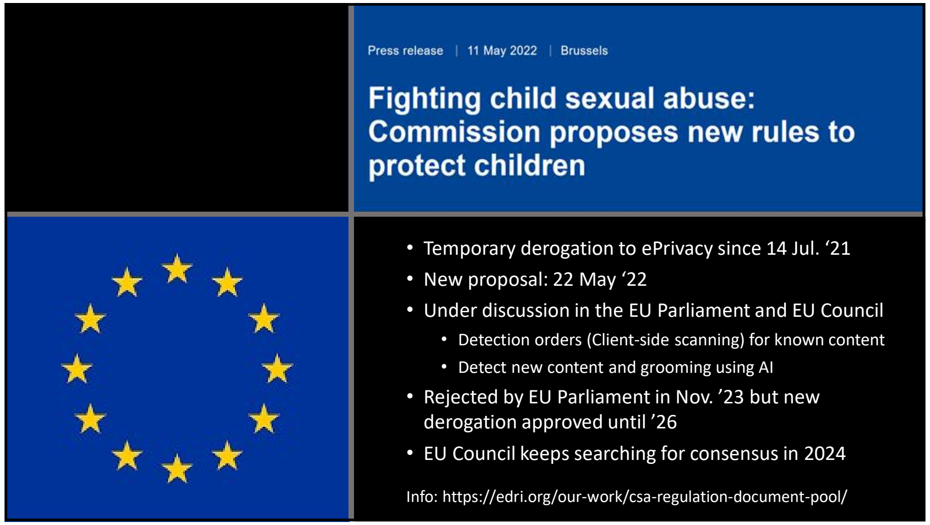
29



The CSAM story (Child Sexual Abuse Material)

- Driven by NCMEC (US) and Thorn
- Detects CSAM content
  - PhotoDNA: secret perceptual hash function
  - secret list of hash values of content
- Many millions of detections per year?
- Threatened by end-to-end encryption

30



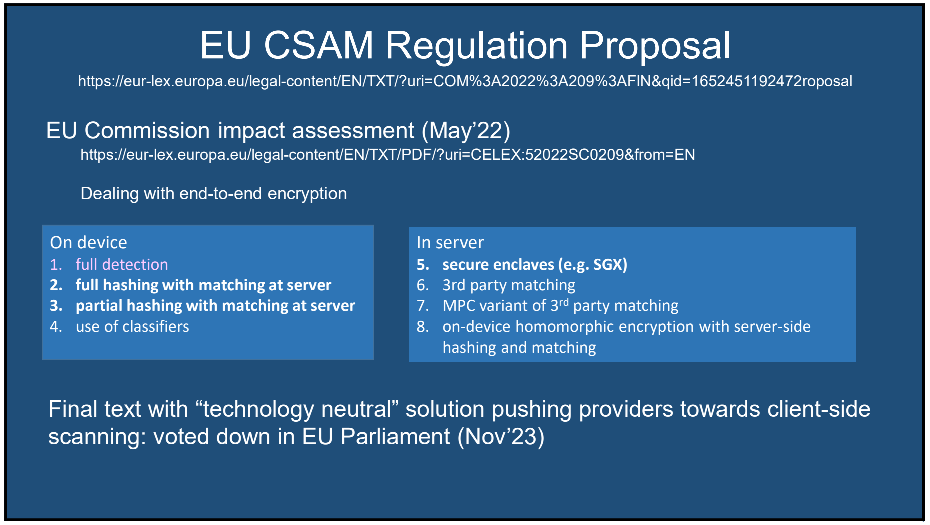
Press release | 11 May 2022 | Brussels

Fighting child sexual abuse: Commission proposes new rules to protect children

- Temporary derogation to ePrivacy since 14 Jul. '21
- New proposal: 22 May '22
- Under discussion in the EU Parliament and EU Council
  - Detection orders (Client-side scanning) for known content
  - Detect new content and grooming using AI
- Rejected by EU Parliament in Nov. '23 but new derogation approved until '26
- EU Council keeps searching for consensus in 2024

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

31



EU CSAM Regulation Proposal

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

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
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

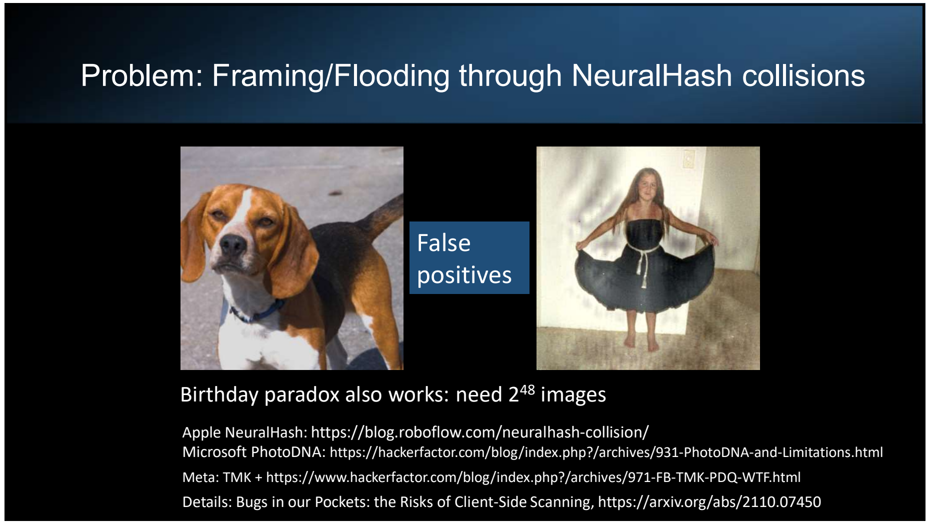
Final text with "technology neutral" solution pushing providers towards client-side scanning: voted down in EU Parliament (Nov'23)

32

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

33

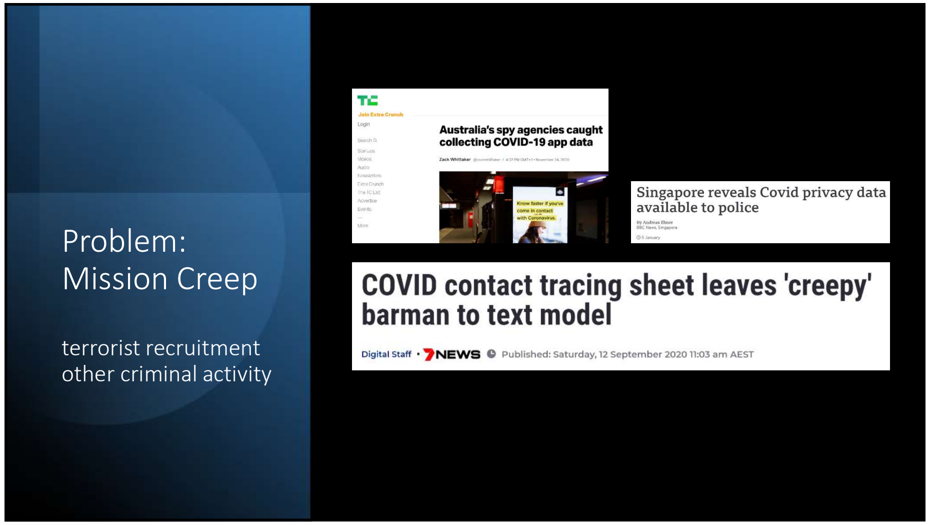


Problem: Framing/Flooding through NeuralHash collisions

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

34



Problem:
Mission Creep

terrorist recruitment
other criminal activity

Australia's spy agencies caught collecting COVID-19 app data

Zack Whittaker @zackwhittaker / 4:32 PM GMT+1 • November 24, 2020

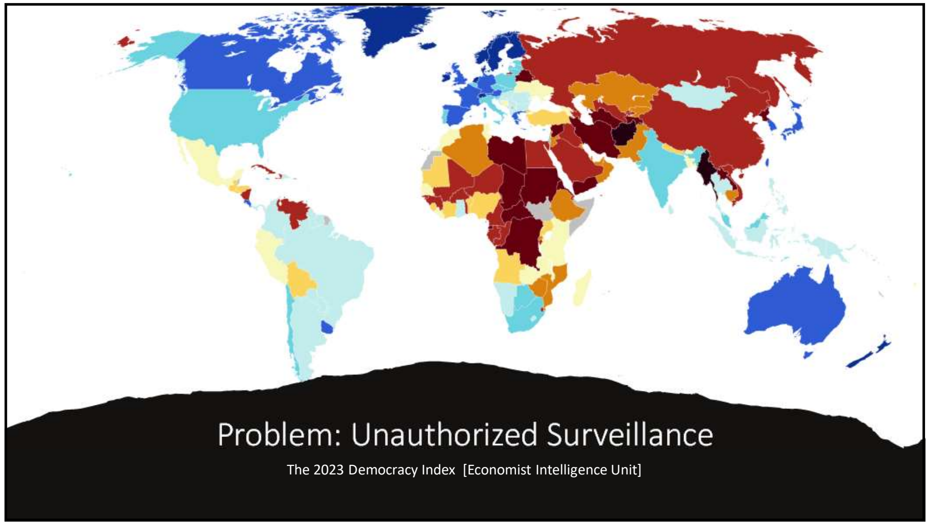
Singapore reveals Covid privacy data available to police

By Andreas Illmer
BBC News, Singapore
5 January

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

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

35



Problem: Unauthorized Surveillance

The 2023 Democracy Index [Economist Intelligence Unit]

36

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. It will undermine security
3. Function creep: terrorism and organized crime
4. It will be abused by (wannabe) dictators
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

Latest changes (June ‘24) (EU Council)

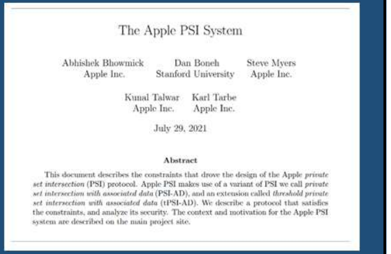
1. Risk levels – services that matter will be high risk
2. No detection of grooming in audio or text
3. At least 2 images for new CSAM - makes no difference
4. Upload moderation with “consent”
5. “We protect end-to-end encryption” - really

37

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…



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.

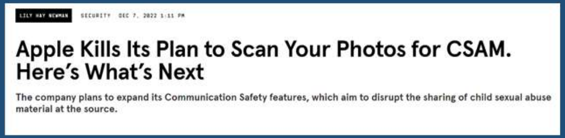
- Needs perceptual hash function: NeuralHash (96 bits)

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

38

Update on Apple’s PSI protocol

[Dec’22]

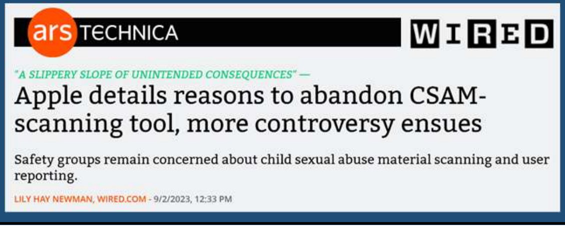


LILY HAY NEWMAN SECURITY DEC 7, 2022 1:11 PM

Apple Kills Its Plan to Scan Your Photos for CSAM. Here’s What’s Next

The company plans to expand its Communication Safety features, which aim to disrupt the sharing of child sexual abuse material at the source.

[Sep’23]



“A SLIPPERY SLOPE OF UNINTENDED CONSEQUENCES” —

Apple details reasons to abandon CSAM-scanning tool, more controversy ensues

Safety groups remain concerned about child sexual abuse material scanning and user reporting.

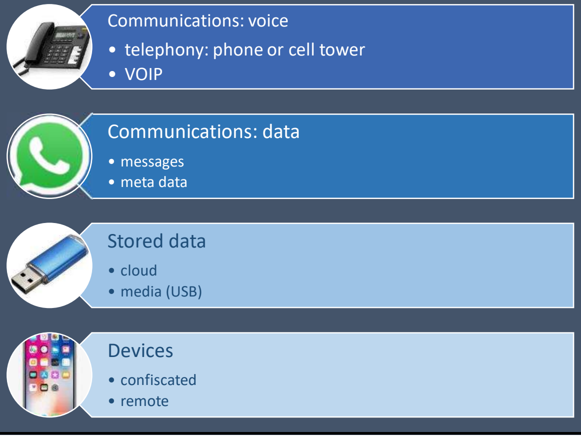
LILY HAY NEWMAN, WIRED.COM - 9/2/2023, 12:33 PM

39

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

40

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

41

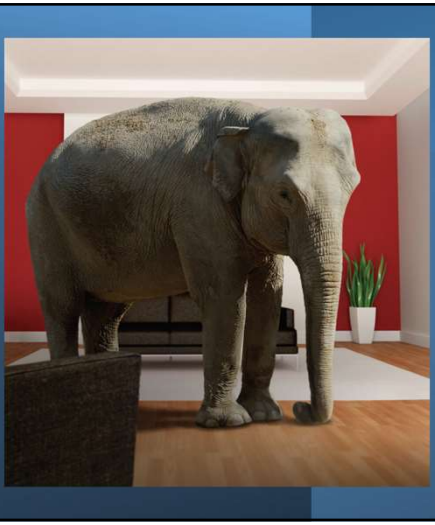
Options for Law Enforcement

- **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**

42

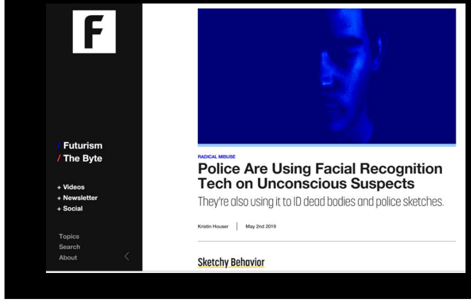
metadata

Law enforcement: metadata is insufficient



43

AI?



F

/ Futurism
/ The Byte

+ Videos
+ Newsletter
+ Social

Topics
Search
About

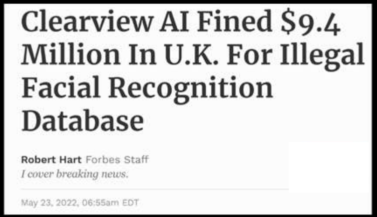
RADICAL MISUSE

Police Are Using Facial Recognition Tech on Unconscious Suspects

They're also using it to ID dead bodies and police sketches.

Kristin Houser | May 2nd 2019

Sketchy Behavior



Clearview AI Fined $9.4 Million In U.K. For Illegal Facial Recognition Database

Robert Hart Forbes Staff
I cover breaking news.

May 23, 2022, 06:55am EDT

44

Options for Law Enforcement: hacking

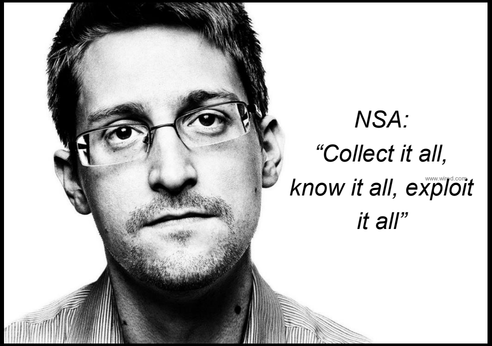
We believe that fighting crime should be easy: we provide effective, easy-to-use offensive technology to the worldwide law enforcement and intelligence communities

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

DE: Bundestrojaner: key logger, screenshots, Skype calls

45

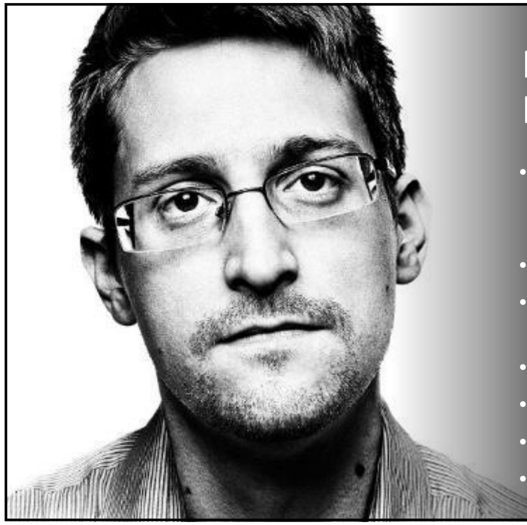
Options for Law Enforcement



NSA: "Collect it all, know it all, exploit it all"

Collaborate with intelligence services

46

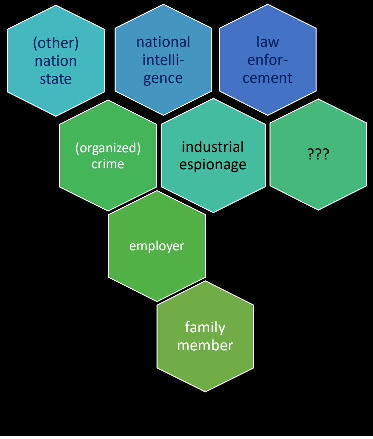


Response of the NSA after 1994

- 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

47

The bigger picture



(other) nation state

national intelli-gence

law enfor-cement

(organized) crime

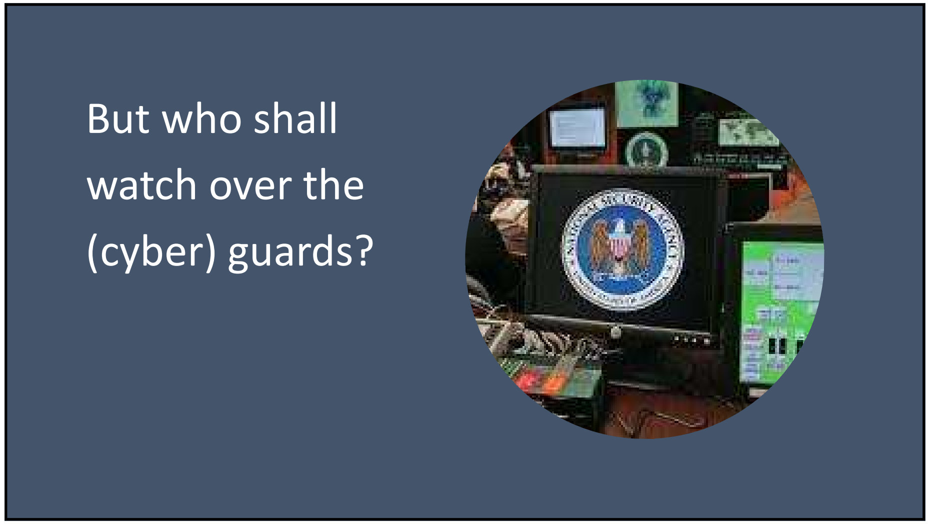
industrial espionage

???

employer

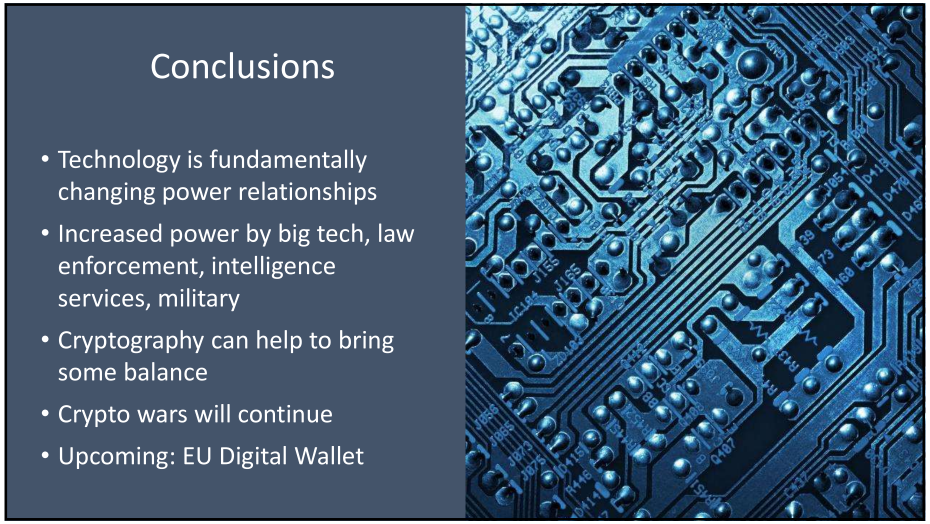
family member

48



But who shall watch over the (cyber) guards?

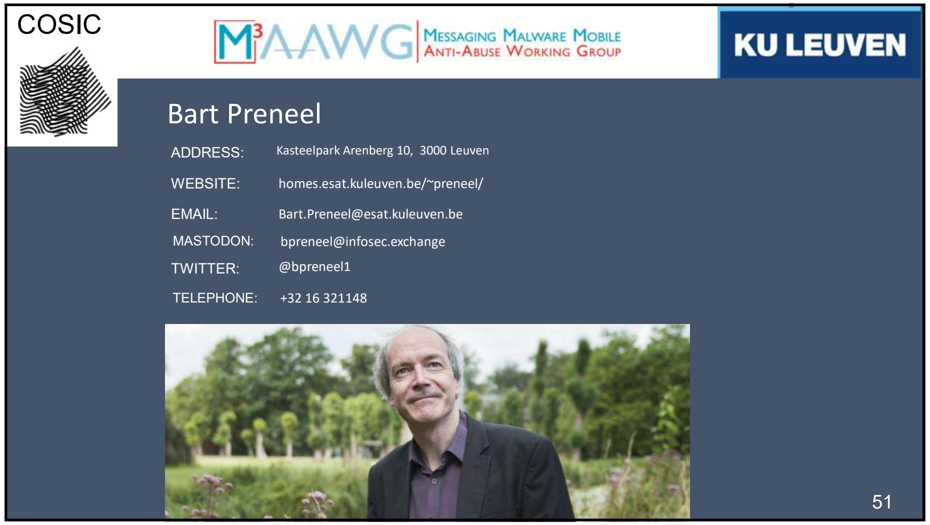
49



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

50



COSIC

M3AAWG Messaging Malware Mobile Anti-Abuse Working Group

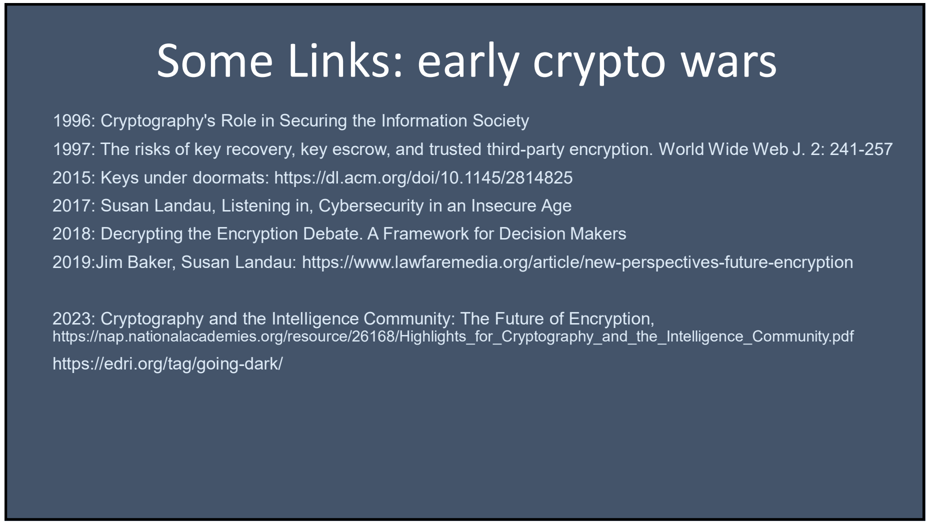
KU LEUVEN

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

51

51

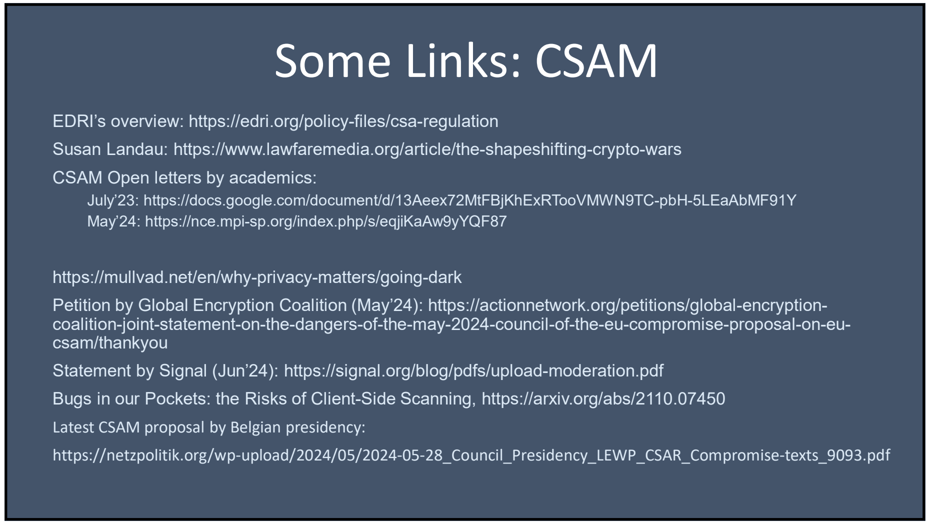


Some Links: early crypto wars

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/

52



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

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

53