



Crypto Policy:
from CSAM to eIDAS

Bart Preneel
@bpreneel1 - preneel@infosec.exchange
5 June 2024

KU LEUVEN
ArenBerg
Crypto BV

COSIC

The slide features a central illustration of a multi-headed, bearded figure with glowing eyes, surrounded by various cryptographic symbols like keys, coins, and a hammer. The background is a gradient of blue and green.

1

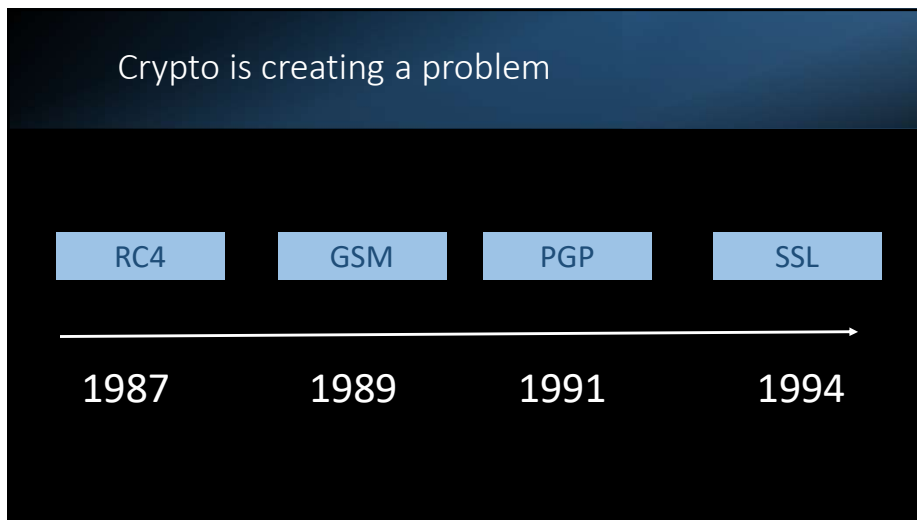


Crypto is creating a problem

I mean
cryptography, not
cryptocurrencies

The slide has a dark blue background with a light blue speech bubble containing the text.

2



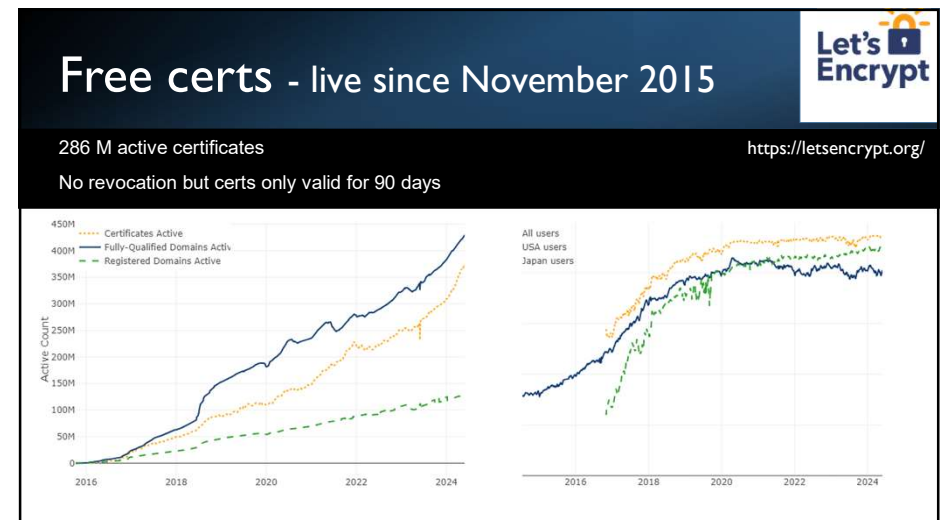
Crypto is creating a problem

RC4 GSM PGP SSL

1987 1989 1991 1994

The slide shows a horizontal timeline with four blue boxes labeled RC4, GSM, PGP, and SSL, positioned above the years 1987, 1989, 1991, and 1994 respectively. A white arrow points from left to right across the timeline.

3



Free certs - live since November 2015

286 M active certificates
No revocation but certs only valid for 90 days

<https://letsencrypt.org/>

Let's Encrypt

Active Count

450M
400M
350M
300M
250M
200M
150M
100M
50M
0

2016 2018 2020 2022 2024

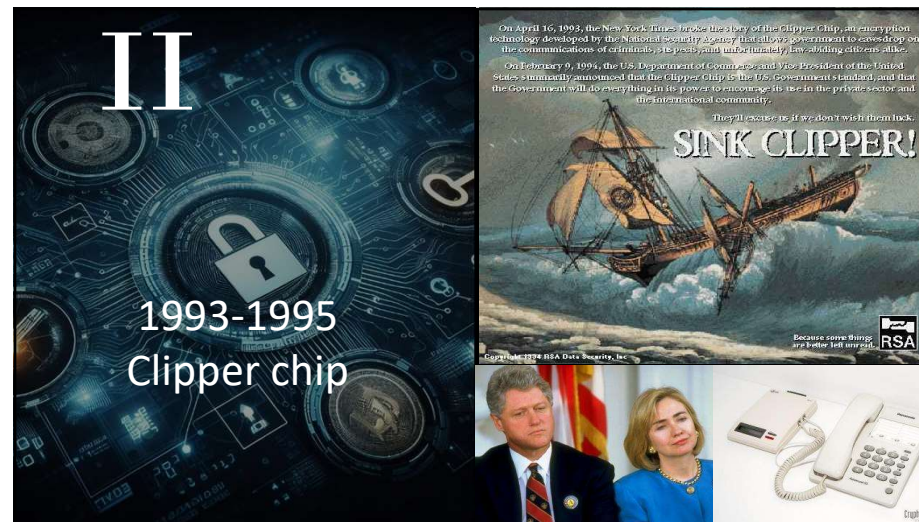
All users
USA users
Japan users

The slide contains two line graphs. The left graph shows 'Active Count' from 2016 to 2024 for 'Certificates Active' (yellow dotted line), 'Fully-Qualified Domains Active' (blue solid line), and 'Registered Domains Active' (green dashed line). The right graph shows 'Active Count' from 2016 to 2024 for 'All users' (blue solid line), 'USA users' (yellow dotted line), and 'Japan users' (green dashed line). The Let's Encrypt logo is in the top right corner.

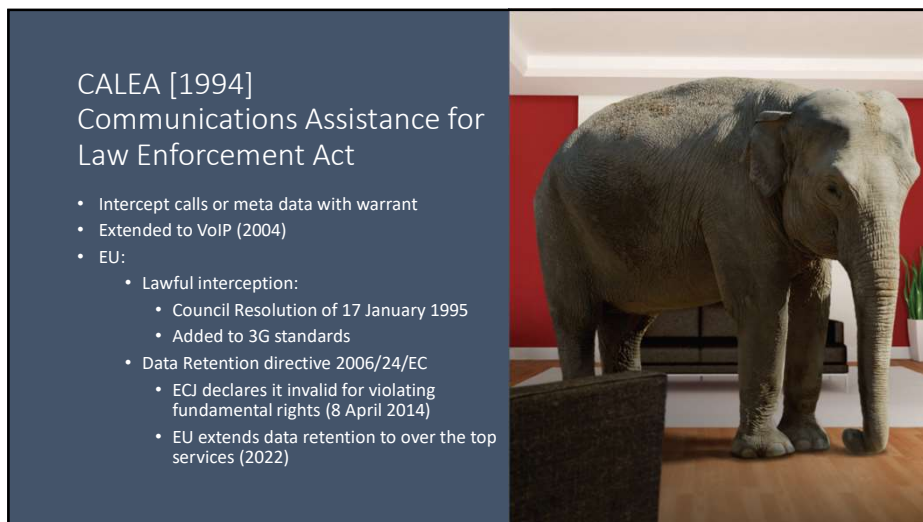
4



5



6



7



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

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

WASHINGTON | BY RICHARD COWAN



U.S. President Barack Obama in Bavaria, Germany on June 8, 2015. REUTERS/KORN LIAWAGIIE

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]

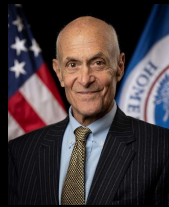
The US is "better served by stronger encryption, rather than baking in weaker encryption,"

"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

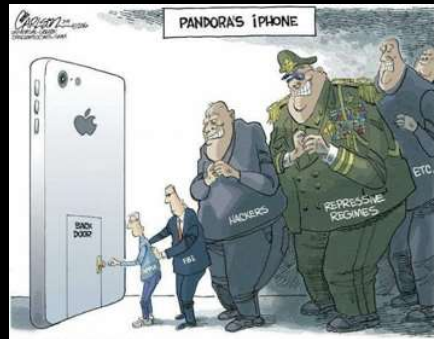
At the request of the FBI, based on an all writs order (1789), a U.S. federal magistrate judge has ordered Apple to break the security of the iPhone



16

The many problems of a backdoor

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



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

17

18

Netherlands (2016)



Ansip: 'I am strongly against any backdoor to encrypted systems'

Home | Digital | Interviews
By Jorge Valero reporting from Barcelona Feb 23, 2016 (updated: Feb 23, 2016)



SECTION SUPPORTERS

HUAWEI

ADVERTISING

FOR A BETTER CONNECTED EUROPE

ENISA Report December 2016: <https://www.enisa.europa.eu/news/enisa-news/the-importance-of-cryptography-for-the-digital-society>

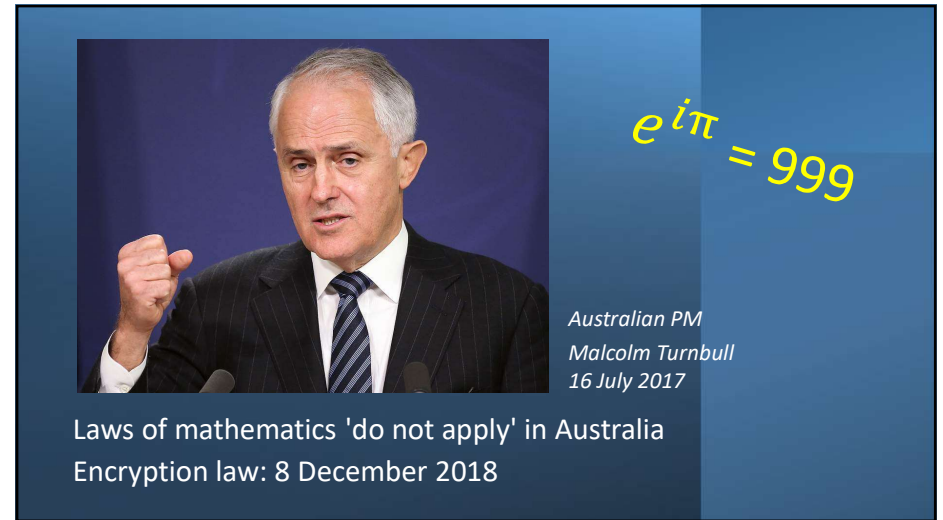
19

20



France and Germany push for encryption limits (2016)

21



$e^{i\pi} = -1$

Australian PM
Malcolm Turnbull
16 July 2017

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

22

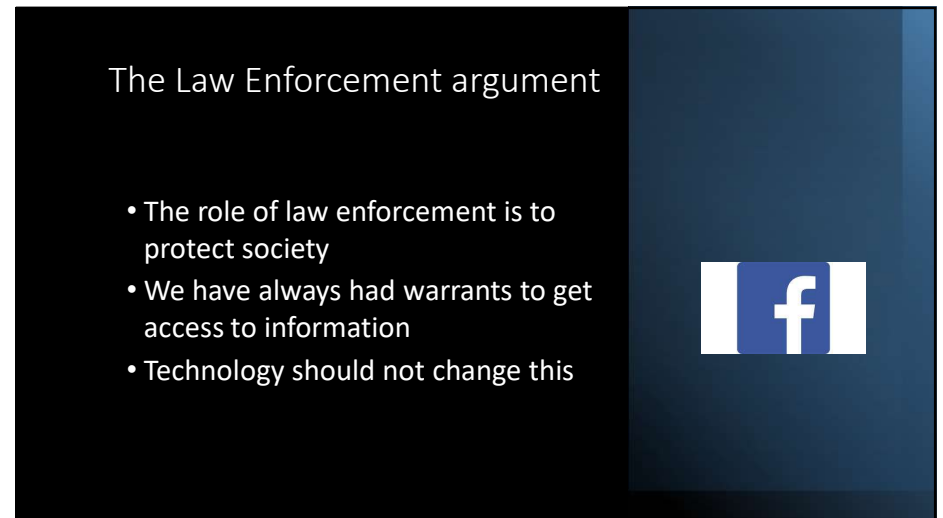


"Warrant-proof encryption defeats the constitutional balance by elevating privacy above public safety,"

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

Deputy attorney general
Rod Rosenstein
9 Nov. 2017

23



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



24

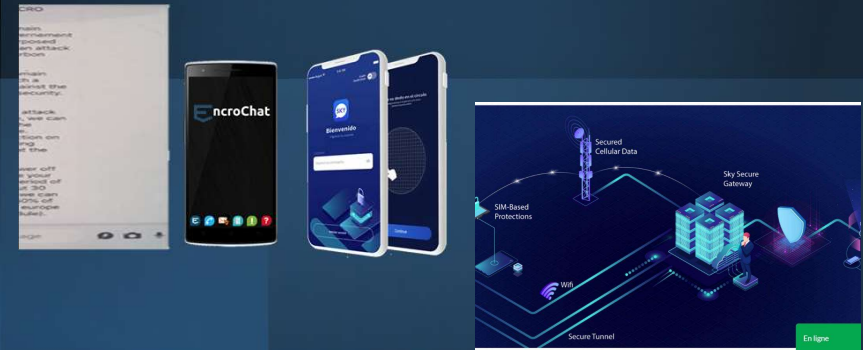
The Law Enforcement argument

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



25

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



26

Can cryptography solve the problem created by cryptography?



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.

27

28

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/>

29

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

30

IV

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



31

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 [...]

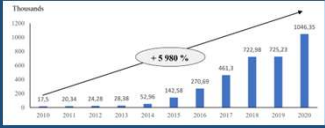
32

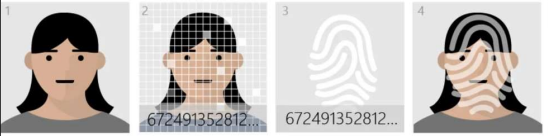
8


The CSAM story (Child Abuse Sexual 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











The Next Chapter in Protecting Children Online



33

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 Feb. '24 but new derogation approved until '26
- Belgian presidency keeps searching for consensus in June '24

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

34

EU CSAM Regulation Proposal

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

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	In server
<ol style="list-style-type: none"> 1. full detection 2. full hashing with matching at server 3. partial hashing with matching at server 4. use of classifiers 	<ol style="list-style-type: none"> 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

35

EU CSAM Regulation Proposal

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

EU Parliament complementary impact assessment (April '23)
[https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU\(2023\)740248](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 (May '24)

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. "We protect end-to-end encryption" - really

36


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



37

Problem: Framing/Flooding through NeuralHash collisions



False positives

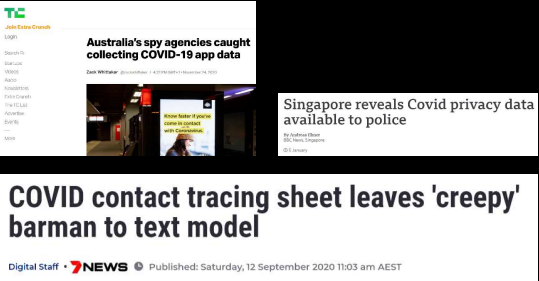
Birthday paradox also works: need 2^{48} images

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>

38

Problem: Mission Creep

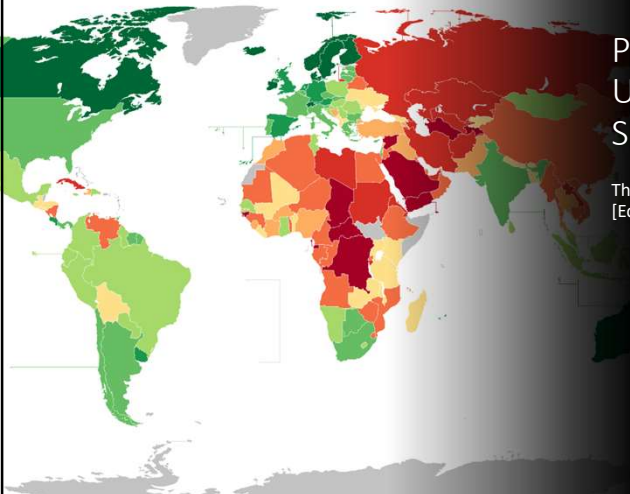
terrorist recruitment
other criminal activity



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


39

Problem: Unauthorized Surveillance



The 2018 Democracy Index [Economist Intelligence Unit]

40



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...
- Needs perceptual hash function: NeuralHash (96 bits)

The Apple PSI System

Abhishek Bhavnick Dan Boneh Steve Myers
Apple Inc. Stanford University Apple Inc.

Kunal Talwar Karl Tarpe
Apple Inc. Apple Inc.

July 29, 2021

Abstract

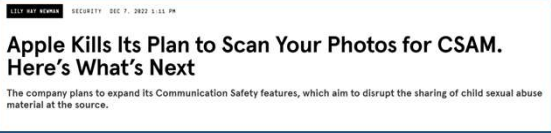
This document describes the constraints that drove the design of the Apple private set intersection (PSI) protocol. Apple PSI makes use of a variant of PSI we call *private set intersection with associated data (PSI-AD)*, and an extension called *threshold private set intersection with associated data (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.

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>

41



Update on Apple's PSI protocol

[Dec'22]  **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]  **Apple details reasons to abandon CSAM-scanning tool, more controversy ensues**
Safety groups remain concerned about child sexual abuse material scanning and user reporting.

42

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

43

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

44


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**

45


metadata

Law enforcement: metadata is insufficient



46

AI?



F

Futurism
The Byte


- Videos
- Newsletter
- Social

Topics
Research
About

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, 06:56am EDT



Police Are Using Facial Recognition Tech on Unconscious Suspects
They're also using it to ID dead bodies and police sketches.

Kevin Hester | May 2nd 2019

Sketchy Behavior

47

Options for Law Enforcement: hacking



NSO GROUP

Cellebrite Digital Intelligence for a safer world.

Remote Control System

Rely on us.

Hacked in 2015

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

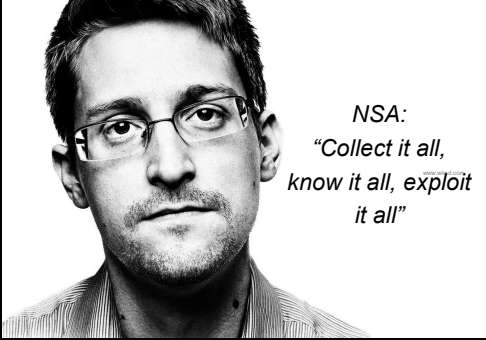


exploit known and unknown vulnerabilities (0-days) to get access

DE: Bundestrojaner: key logger, screenshots, Skype calls

48

Options for Law Enforcement



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

Collaborate
with
intelligence
services

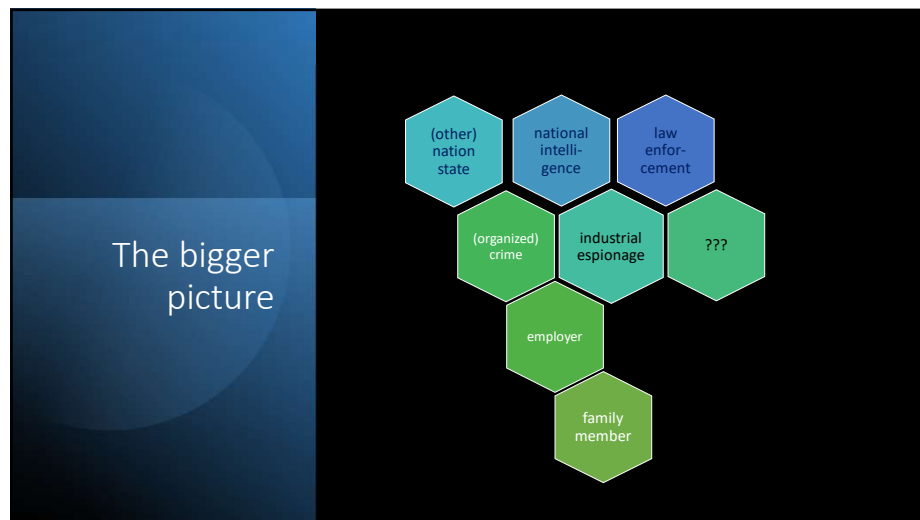
49



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

50



51

But who shall watch over the (cyber) guards?



52



THE GOOD, THE BAD,
AND THE UGLY

Part 2 eIDAS 2.0 regulation

53

eIDAS 1.0 (2014): limited uptake

- signatures
- seals
- time stamps
- registered delivery services
- certificates for website authentication (QWACs)
- preservation of signatures & seals

But

- mostly public sector (limited use in private sector)
- few providers
- inflexible
- not cross-border: member state implementations

54

eIDAS 2.0 (announced June'21):

- certificates for website authentication update
- mobile identity wallet with government-issued identities
 - but also additional attributes (public and private issued)
 - selective disclosure of attributes
- electronic ledgers
- ...

55

In force 20 May 2024



- **digital identity wallet** available and recognized by 2026
 - one per member state
- remains **voluntary** (avoid discrimination if non-use)
- **qualified website authentication certificates (QWACs)**

56

The Good

- interoperable at EU level (technical but not semantical)
 - Architecture Reference Framework
 - <https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline>
 - <https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/discussions>
- open source implementation
- privacy focus:
 - no unique identifier for all applications
 - preclude tracking, profiling and discrimination
 - registration of relying parties

57

The Bad: linkability

- server side likely not open source
 - member states are granted leeway so that, for justified reasons, specific components other than those installed on user devices need not be disclosed
- The technical framework of the European Digital Identity Wallet shall **not allow** providers of electronic attestations of attributes or any other party, after the issuance of the attestation of attributes, **to obtain data that allows for tracking, linking, correlating or otherwise obtain knowledge of transactions or user behaviour unless explicitly authorised by the user.**
- unlinkability and unobservability (w.r.t. service provider) **optional: migration of service providers to weakest Member State**
- ARF not up to date (public: 1.3)
 - technical implementation unclear
 - anonymous credentials (1985) seen as too innovative: only one-time use credentials

58

The Ugly: impact on WebPKI 1/5

Browser user trusts all 660 CAs in the browser
Adding CAs = at best not reducing security

59

The Ugly: impact on WebPKI 2/5

- eIDAS 2.0 further pushes for QWACS (Qualified Web Authentication Certificates) issued by QTSPs
- showing legal identity to user in a user-friendly way
- tried before (2008-2016) and abandoned in WebPKI: under the name Extended Validation
- problems
 - companies may have 5+ legal entities in Europe (BV, Srl, GmbH,...)
 - researchers registered a company with as name "Identity Verified"

Insanity Is Doing the Same Thing Over and Over Again and Expecting Different Results

60

The Ugly: QWACS/QTSPs last minute changes 3/5

- do the current 53 QTSPs comply with (free) certification processes? (data from Mozilla)
 - 23 YES
 - 17 never applied
 - 5 in queue
 - 8 failed and did not reapply
- what does eIDAS 2.0 say:
 - Root keys of accredited CAs of Member States need to be inserted in browser trust store
- Art. 45: “browsers to recognise any certificate that satisfies some criteria specified in regulation, *without any other requirements to be imposed by the browsers*”
- will certificate transparency be allowed? Other new ideas?
- opens door for
 - person-in-the-middle attack by EU Member states
 - similar attacks by other (less democratic) countries
- do we trust ETSI?

61

The Ugly: last minute changes 4/5

After 2nd open letter (Oct. 23): Recital 32 was updated (refusal to update Art. 45)

“Recognition of QWACs means that the providers of web-browsers should not deny the authenticity of qualified certificates for website authentication for the sole purpose of attesting the link between the website domain name and the natural or legal person to whom the certificate is issued and confirming the identity of that person.

The obligation of recognition, interoperability and support of QWACs is not to affect the freedom of web-browser providers to ensure web security, domain authentication and the encryption of web traffic in the manner and with the technology they consider most appropriate.”

62

The Ugly last minute changes 5/5

Mitigation of Art. 45

“By way of derogation to paragraph 1 and only in case of substantiated concerns related to breaches of security or loss of integrity of an identified certificate or set of certificates, web-browsers may take precautionary measures in relation to that certificate or set of certificates.”

Supervisory authority and European Commission notified of concerns

Supervisory authority then decides whether or not the certificates have to be reinstated

Note: Article 4 of the Lisbon treaty allows for national security exception

63

Timeline

<https://www.europarl.europa.eu/legislative-train/spotlight-JD22/file-eid>

- Commission proposal: 3 June 2021
- EU Parliament ITRE: 9 February 2022
- First open letter (39 scientists): 2 March 2022
- EU Parliament ITRE: 16 March 2022
- Trilogue start: 21 March 2023
- Trilogue provisional agreement: June 2023 (secret)
- Second open letter (550+ scientists and 40+ NGOs) after leak: 2 November 2023
- End of trilogue: 8 November 2023
- Statement: still concerns (80+ scientists): 23 November 2023
 - Request for additional statement clarifying the recital and the unlinkability
- EU Parliament ITRE vote: 28 November 2023 but postponed till 7 December due to “technical error”
- Full Parliament vote: 29 February 2024
- Adoption by Council: 26 March 2024
- In force: 20 May 2024

64



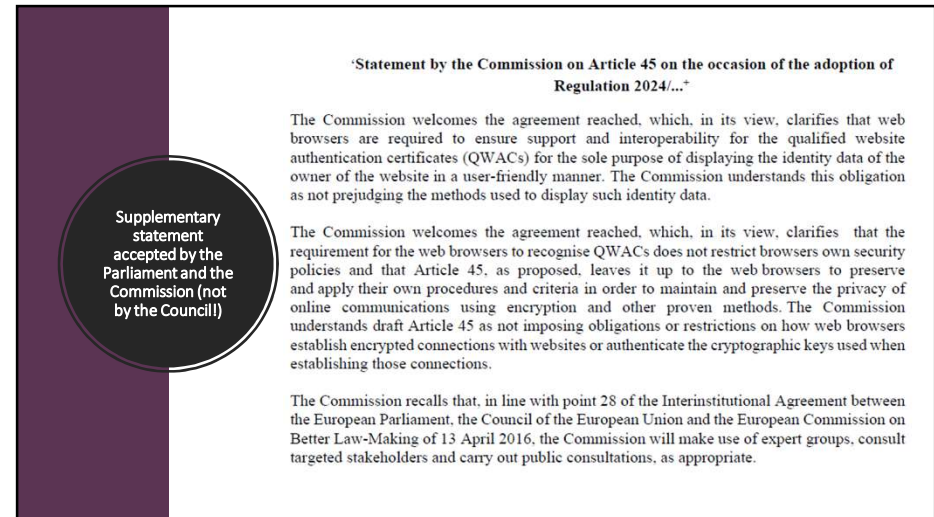
European Council
Council of the European Union

[Home](#) > [Press](#) > [Press releases](#)

Council of the EU | Press release | 26 March 2024 10:30

European digital identity (eID): Council adopts legal framework on a secure and trustworthy digital wallet for all Europeans

65



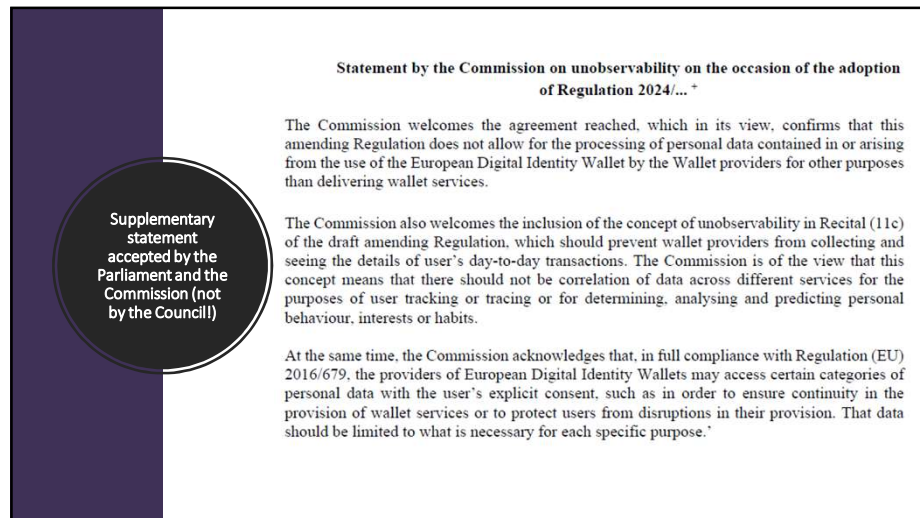
Statement by the Commission on Article 45 on the occasion of the adoption of Regulation 2024/...⁺

The Commission welcomes the agreement reached, which, in its view, clarifies that web browsers are required to ensure support and interoperability for the qualified website authentication certificates (QWACs) for the sole purpose of displaying the identity data of the owner of the website in a user-friendly manner. The Commission understands this obligation as not prejudging the methods used to display such identity data.

The Commission welcomes the agreement reached, which, in its view, clarifies that the requirement for the web browsers to recognise QWACs does not restrict browsers own security policies and that Article 45, as proposed, leaves it up to the web browsers to preserve and apply their own procedures and criteria in order to maintain and preserve the privacy of online communications using encryption and other proven methods. The Commission understands draft Article 45 as not imposing obligations or restrictions on how web browsers establish encrypted connections with websites or authenticate the cryptographic keys used when establishing those connections.

The Commission recalls that, in line with point 28 of the Interinstitutional Agreement between the European Parliament, the Council of the European Union and the European Commission on Better Law-Making of 13 April 2016, the Commission will make use of expert groups, consult targeted stakeholders and carry out public consultations, as appropriate.

66



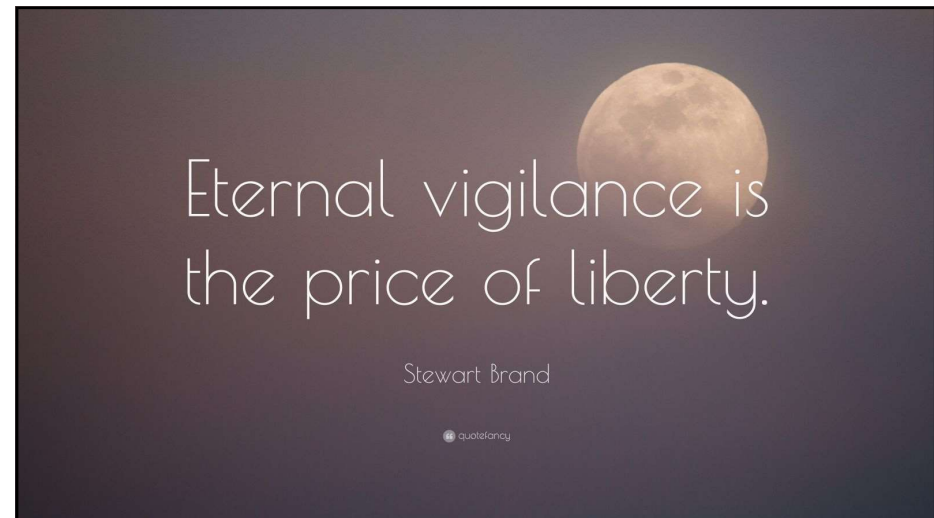
Statement by the Commission on unobservability on the occasion of the adoption of Regulation 2024/...⁺

The Commission welcomes the agreement reached, which in its view, confirms that this amending Regulation does not allow for the processing of personal data contained in or arising from the use of the European Digital Identity Wallet by the Wallet providers for other purposes than delivering wallet services.

The Commission also welcomes the inclusion of the concept of unobservability in Recital (11c) of the draft amending Regulation, which should prevent wallet providers from collecting and seeing the details of user's day-to-day transactions. The Commission is of the view that this concept means that there should not be correlation of data across different services for the purposes of user tracking or tracing or for determining, analysing and predicting personal behaviour, interests or habits.

At the same time, the Commission acknowledges that, in full compliance with Regulation (EU) 2016/679, the providers of European Digital Identity Wallets may access certain categories of personal data with the user's explicit consent, such as in order to ensure continuity in the provision of wallet services or to protect users from disruptions in their provision. That data should be limited to what is necessary for each specific purpose.¹

67



Eternal vigilance is the price of liberty.

Stewart Brand

quotefancy

68

Conclusions

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



69

Bart Preneel

ADDRESS: Kasteelpark Arenberg 10, 3000 Leuven

WEBSITE: homes.esat.kuleuven.be/~preneel/

EMAIL: Bart.Preneel@esat.kuleuven.be

MASTODON: [bpreneel@infosec.exchange](https://infosec.exchange/@bpreneel)

TWITTER: [@bpreneel1](https://twitter.com/bpreneel1)

TELEPHONE: +32 16 321148



KU LEUVEN

ArenBerg Crypto
BV



COSIC



70

Some Links: CSAM

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

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>

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>

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

71

Some Links: eIDAS

<https://www.europarl.europa.eu/legislative-train/spotlight-JD22/file-eid>

https://www.europarl.europa.eu/doceo/document/TA-9-2024-0117_EN.html (statements by Commission in annex at the end)

Nov' 23

eIDAS 2.0 Draft: <https://www.europarl.europa.eu/cmsdata/278103/eIDAS-4th-column-extract.pdf>

<https://last-chance-for-eidas.org/>

March 22: https://www.eff.org/files/2022/03/02/eidas_cybersecurity_community_open_letter_1_1.pdf

October 23: <https://eidas-open-letter.org>

November 23: <https://eidas-open-letter.org/statement-23-11-2023.pdf>

December 23: <https://eidas-open-letter.org/response-01-12-2023>

Other comment (Ryan Hurst) <https://docs.google.com/document/d/1sGzaE9QTs-gorr4BTqKAe0AaGKjt5GagyEevDoavWU0/edit#heading=h.bknjsqpu0hyu>

72