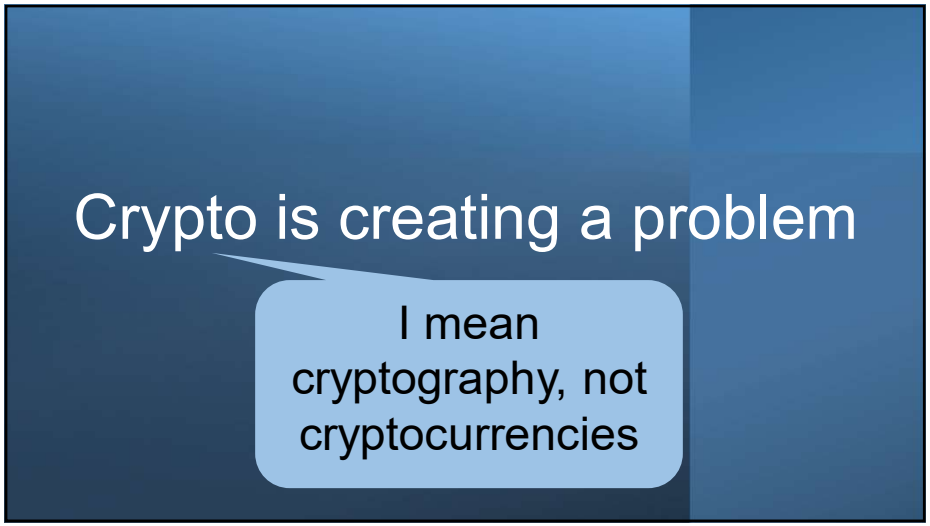
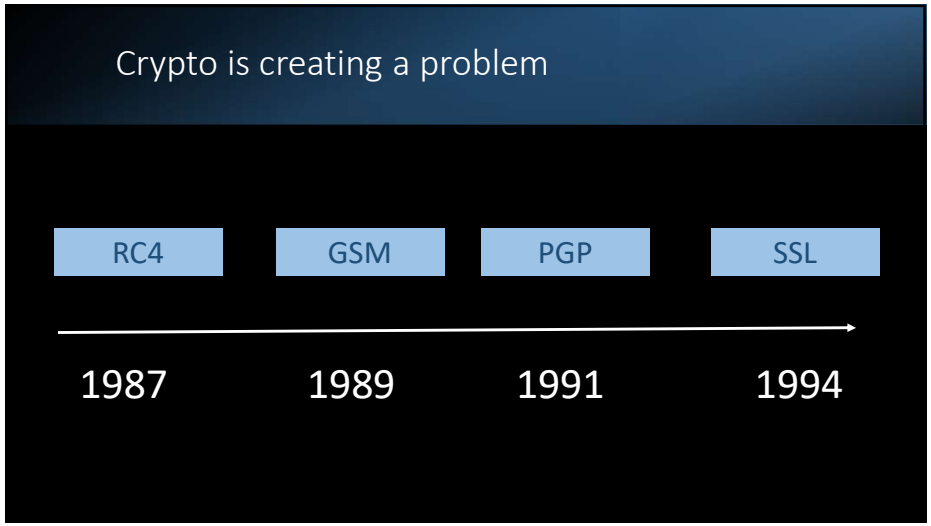

The Many Faces of the Crypto Wars
Bart Preneel
@bpreneel1 - preneel@infosec.exchange
31 May 2024
KU LEUVEN
COSIC
ArenBerg Crypto BV

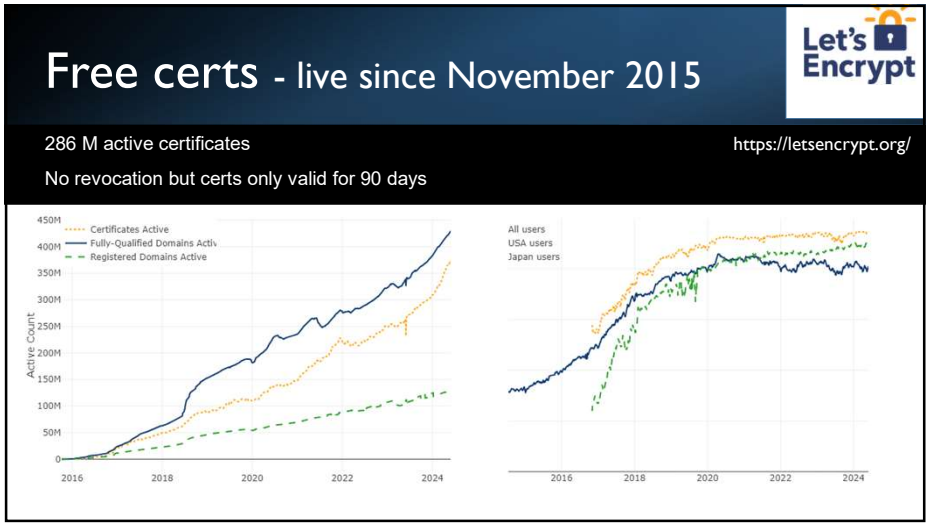
1


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
286 M active certificates
https://letsencrypt.org/
No revocation but certs only valid for 90 days
Certificates Active
Fully-Qualified Domains Activ
Registered Domains Active
Active Count
All users
USA users
Japan users

4

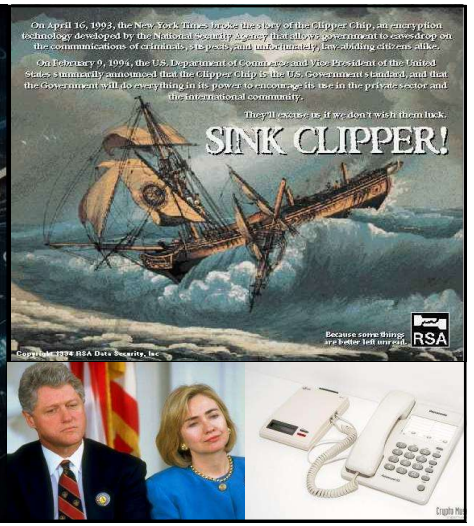
I

1975-1998
stopping
research &
publications

5

II

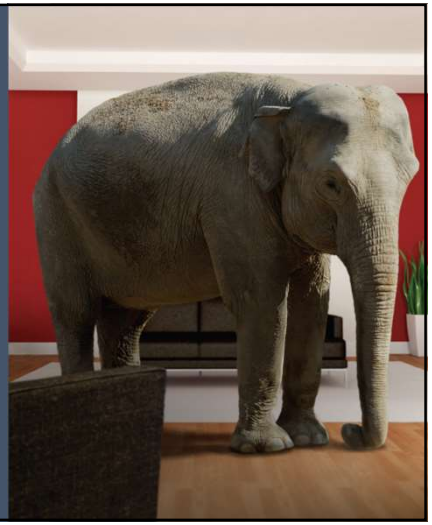
1993-1995
Clipper chip



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 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, CYBERSECUR

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."

Google

Microsoft

IBM

12

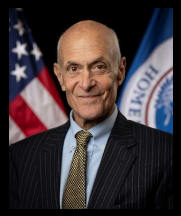
Former NSA/DHS Directors against key escrow [2015]

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
- …

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

Netherlands (2016)


KABINET: GEEN ACHTERDEUR IN ENCRYPTIE

6 JANUARI 2016

19

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

Home | Digital | Interviews

By Jorge Valero reporting from Barcelona

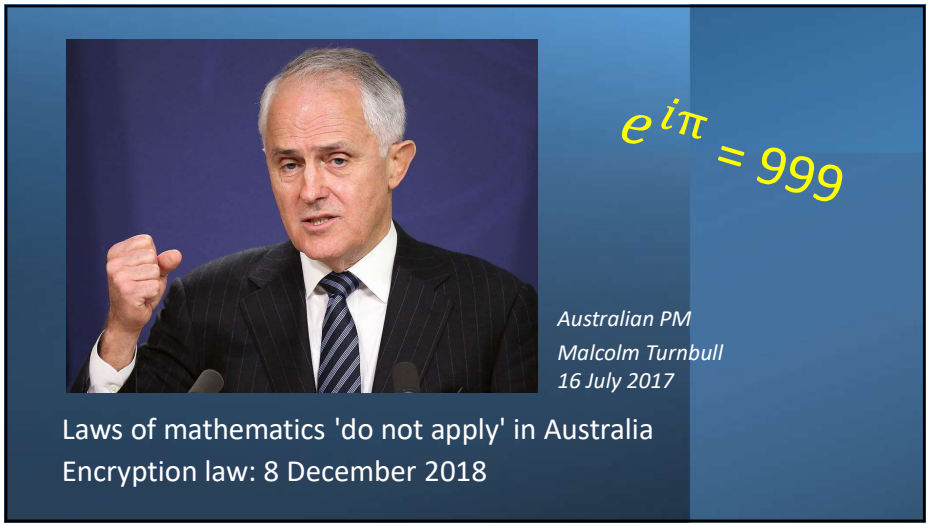
Feb 23, 2016 (updated: Feb 23, 2016)

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

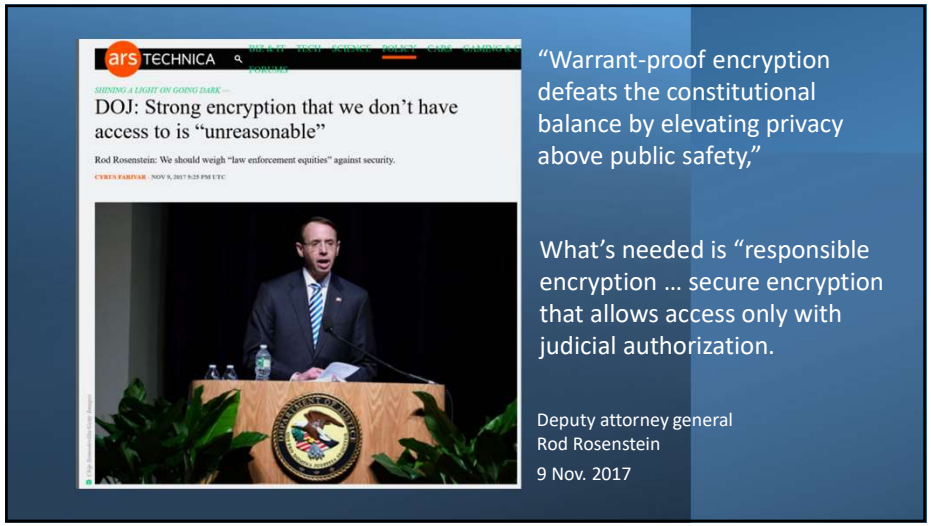
20


France and Germany push
for encryption limits (2016)
Ministère de l'
23 août 20

21


$e^{i\pi} = 999$
Australian PM
Malcolm Turnbull
16 July 2017
Laws of mathematics 'do not apply' in Australia
Encryption law: 8 December 2018

22


ars TECHNICA
DOJ: Strong encryption that we don't have access to is "unreasonable"
Rod Rosenstein: We should weigh "law enforcement equities" against security.
"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


Encrochat ('20) - Sky ECC ('21) – Exclu ('23)
https://www.darkreading.com/endpoint/exclu-shutdown-underscores-outsized-apps-messaging-apps-role-in-cybercrime

24

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/

25

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

26

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

27

Press release | 11 May 2022 | Brussels

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

- Temporary regulation since 14 July 2021
- New proposal: 22 May 2022 – 8 weeks comment
- Under discussion in the EU Parliament and EU Council
- Client side scanning for known content
- Detect new content and grooming using AI

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

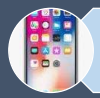
28

Which access is needed?

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

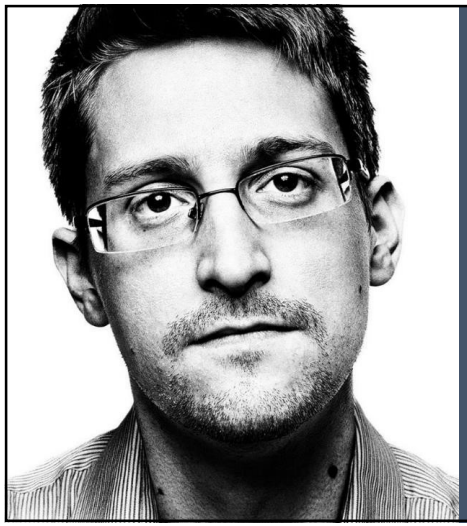
Communications: data
- messages
- meta data

Stored data
- cloud
- media (USB)



Devices
- confiscated
- remote

29

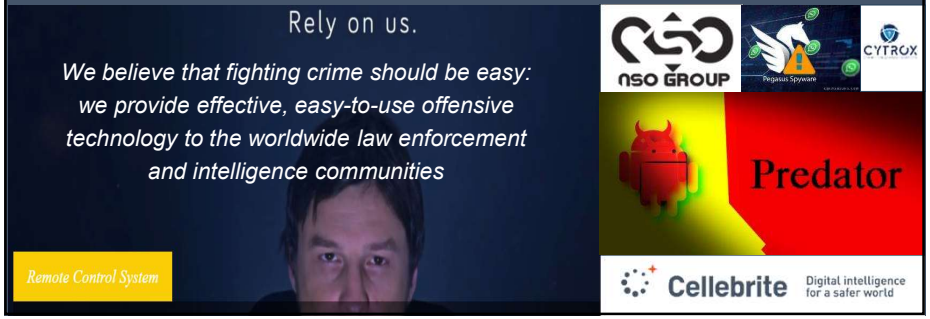


Beyond law enforcement: intelligence services

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

30

Beyond law enforcement: rogue companies and 0-days



31

But who shall watch over the (cyber) guards?

32

Part 2 eIDAS 2.0 regulation

33

eIDAS 1.0 (2014): limited uptake

- signatures
- seals
- time stamps
- registered delivery services
- dertificates 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

34

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
- …

35

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)

36

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

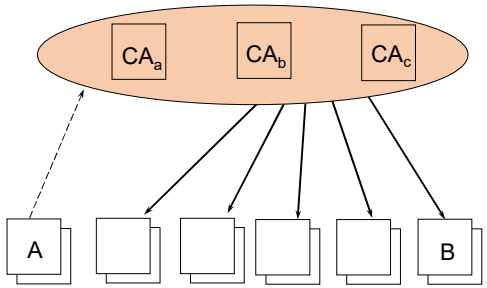
37

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: 1.0)
  - technical implementation unclear
  - anonymous credentials (1985) seen as too innovative: only one-time use credentials

38

The Ugly: impact on WebPKI 1/5



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

39

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

40

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?

41

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."

42

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

43

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

44

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

45

Supplementary statement accepted by the Parliament and the Commission (not by the Council)

'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.

46

Supplementary statement accepted by the Parliament and the Commission (not by the Council)

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.'

47

Eternal vigilance is the price of liberty.

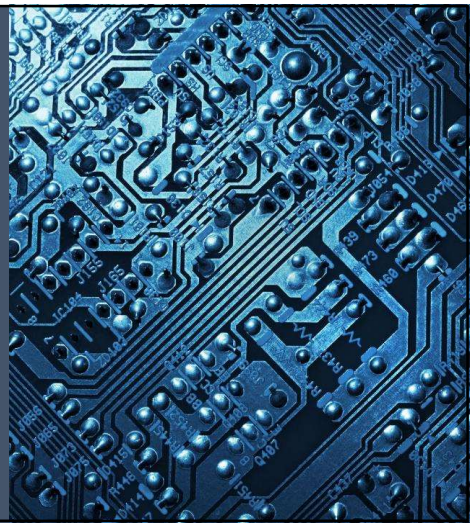
Stewart Brand

quotefancy

48

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

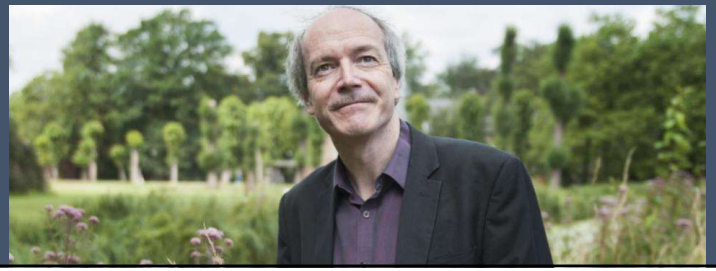


49

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



50

50

Some Links

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-qorr4BTqKAe0AaGKjt5GagyEevDoavWU0/edit#heading=h.bknjsqpu0hyu

51