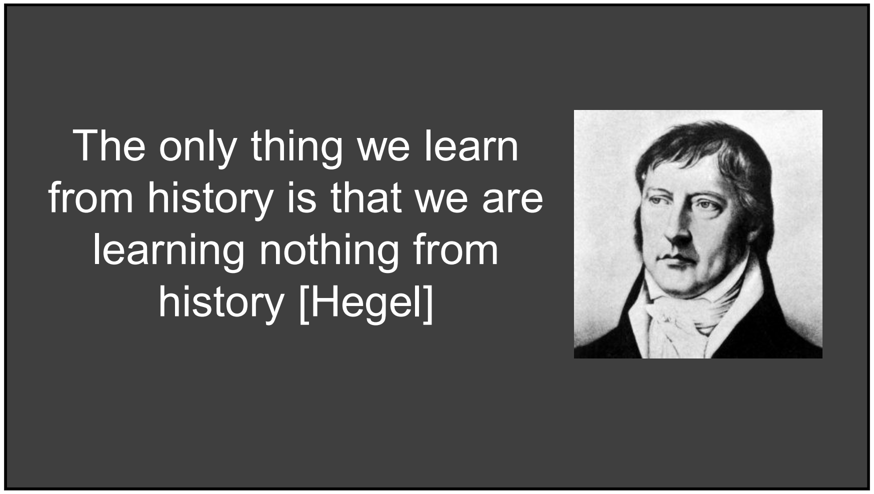
Three decades of cybersecurity policy: Lessons learned

Bart Preneel
COSIC, KU Leuven
@bpreneel1
22 June 2022

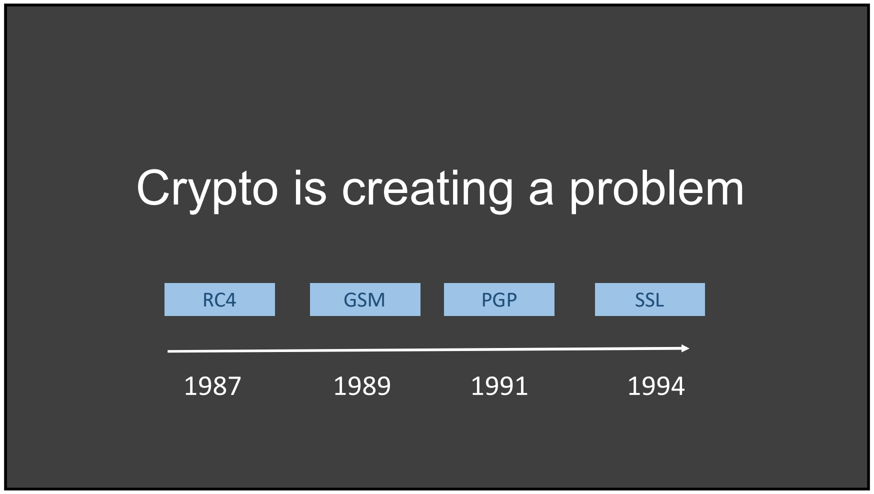
imec
embracing a better life
KU LEUVEN
nextAuth
Best in mobile user authentication
COSIC



The only thing we learn from history is that we are learning nothing from history [Hegel]

Crypto is creating a problem

I mean cryptography, not cryptocurrencies



Crypto is creating a problem

RC4	GSM	PGP	SSL
1987	1989	1991	1994

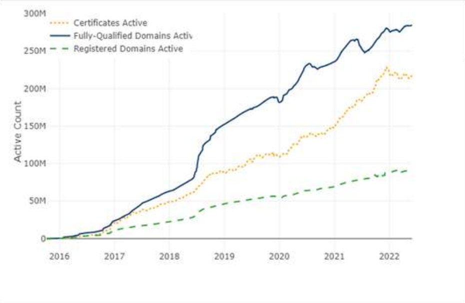
Free certs - live since November 2015

Let's Encrypt

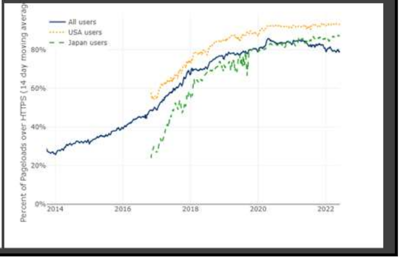
https://letsencrypt.org/

260 M active certificates

No revocation but certs only valid for 90 days



Firefox https

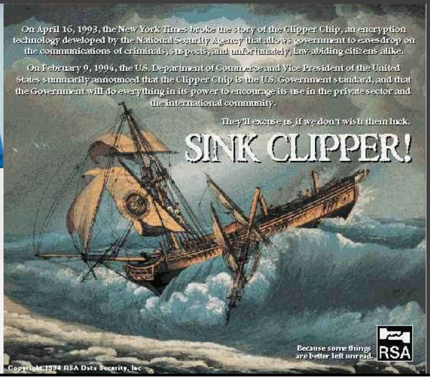


Options for Law Enforcement (1/4)

- **do nothing**
- **use built-in key escrow ("special access" or "backdoor")**
  - key management feature
  - secret sharing
  - functionality inside device that can be activated locally or remotely

Law Enforcement Access

So 1990s



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.

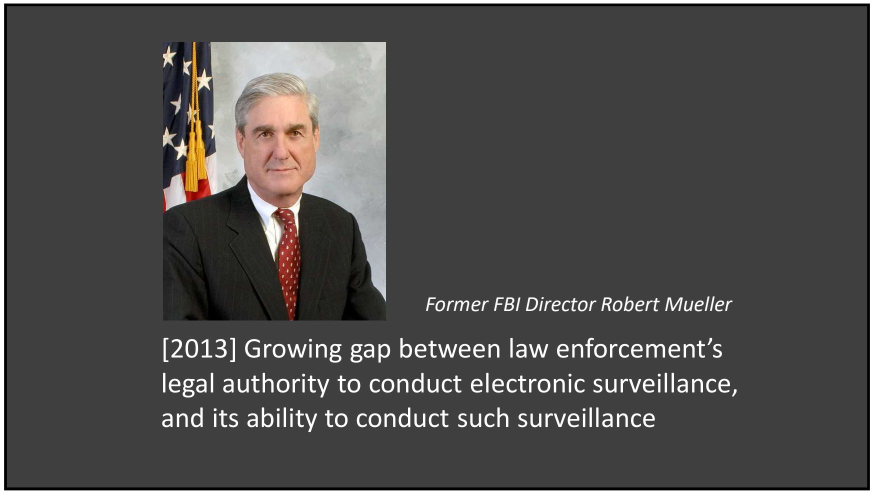
Copyright 1994 RSA Data Security, Inc

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)

France lifted ban on strong encryption in 1999



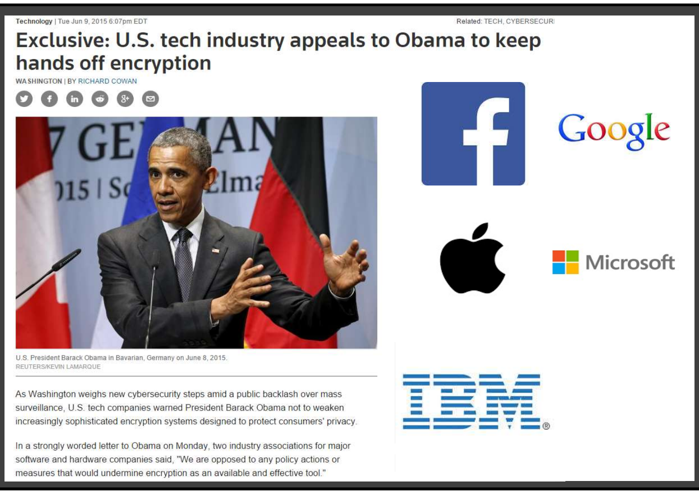
Former FBI Director Robert Mueller

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

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.*

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



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

Related: TECH, CYBERSECURI

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

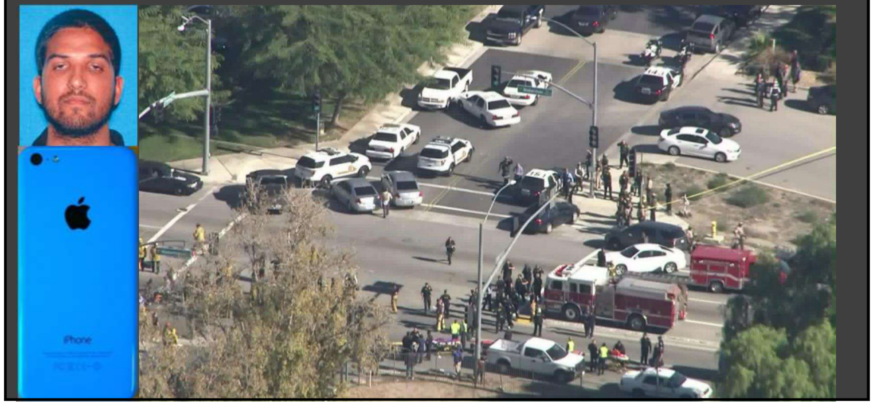
WASHINGTON | BY RICHARD COWAN

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."

San Bernardino, CA, December 2, 2015



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

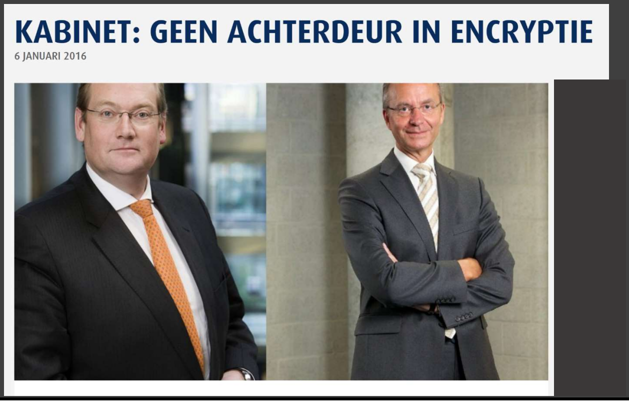
Court case ends

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

…yielded almost no useful information

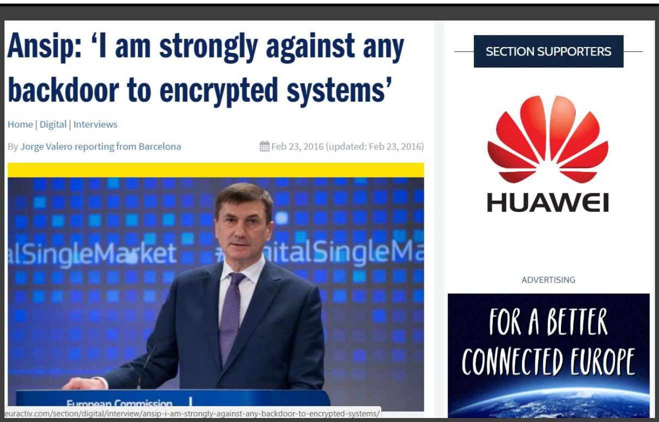
Sept. 2016: Sergei Skorobogatov (Cambridge University) shows that access is feasible with $100 of equipment

Netherlands (2016)



KABINET: GEEN ACHTERDEUR IN ENCRYPTIE

6 JANUARI 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

euractiv.com/section/digital/interview/ansip-i-am-strongly-against-any-backdoor-to-encrypted-systems/

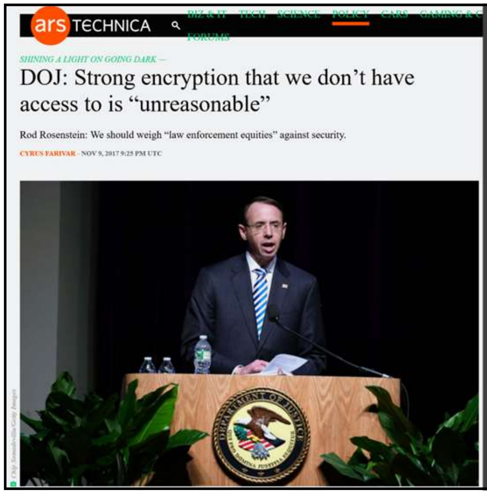
ENISA Report December 2016: https://www.enisa.europa.eu/news/enisa-news/the-importance-of-cryptography-for-the-digital-society

France and Germany push for encryption limits (2016)

$e^{i\pi} = 999$

Australian PM
Malcolm Turnbull
16 July 2017

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



SHINING A LIGHT ON GOING DARK —

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

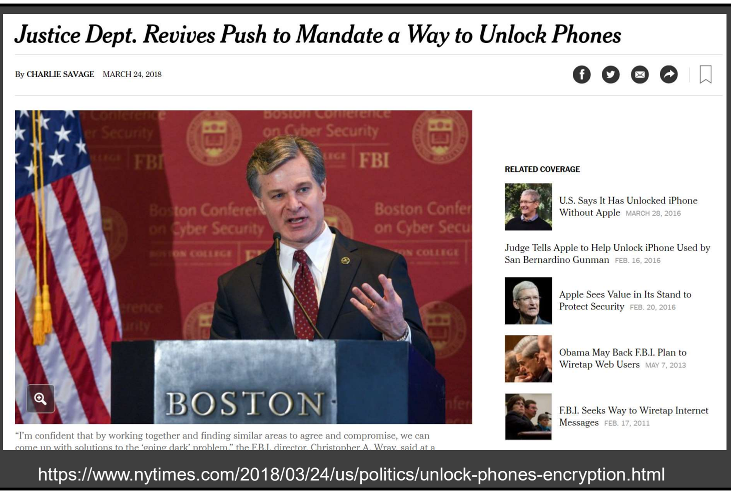
Rod Rosenstein: We should weigh "law enforcement equities" against security.

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



Justice Dept. Revives Push to Mandate a Way to Unlock Phones

By CHARLIE SAVAGE MARCH 24, 2018

"I'm confident that by working together and finding similar areas to agree and compromise, we can come up with solutions to the 'going dark' problem," the F.B.I. director, Christopher A. Wray, said at a

RELATED COVERAGE

U.S. Says It Has Unlocked iPhone Without Apple MARCH 28, 2016

Judge Tells Apple to Help Unlock iPhone Used by San Bernardino Gunman FEB. 16, 2016

Apple Sees Value in Its Stand to Protect Security FEB. 20, 2016

Obama May Back F.B.I. Plan to Wiretap Web Users MAY 7, 2013

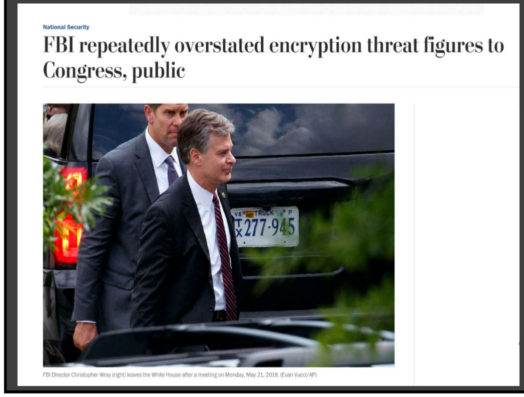
F.B.I. Seeks Way to Wiretap Internet Messages FEB. 17, 2011

https://www.nytimes.com/2018/03/24/us/politics/unlock-phones-encryption.html

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

The Law Enforcement argument



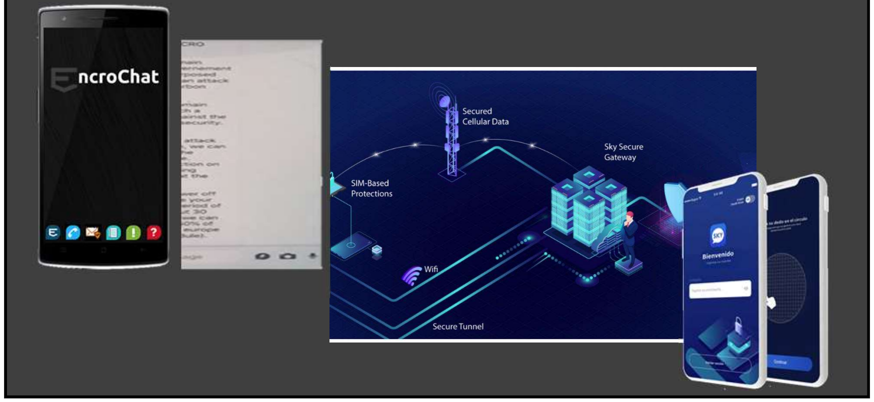
National Security

FBI repeatedly overstated encryption threat figures to Congress, public

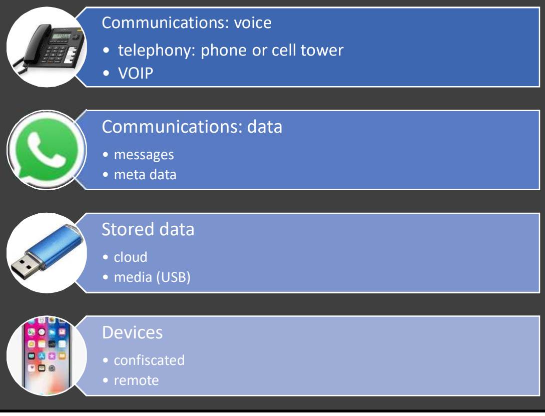
FBI Director Christopher Wray (right) leaves the White House after a meeting on Monday, May 21, 2018. (Evan Vucci/AP)

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

Encrochat (2020) and Sky ECC (2021)



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

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/

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.

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

EU COM(2017)608
towards an effective and genuine Security Union

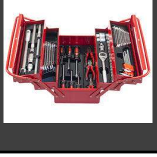
encryption will not be "prohibited, limited or weakened"

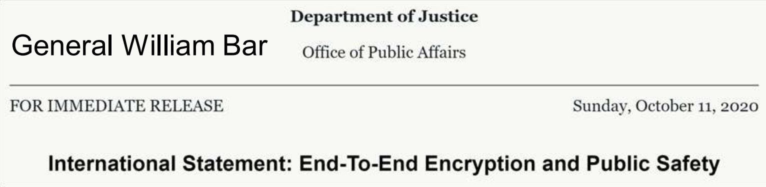
"measures should not have an impact on a larger or indiscriminate number of people".

- more collaboration
- 24 ~~96~~ extra people for Europol

EUROPOL

- encourages the countries to collaborate in developing a toolbox with alternative investigation techniques
  - Key search machines? 0-days? Malware?





General William Bar

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

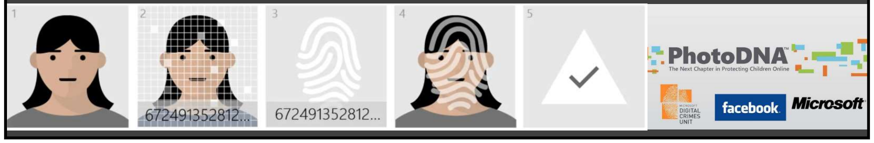
Sunday, October 11, 2020

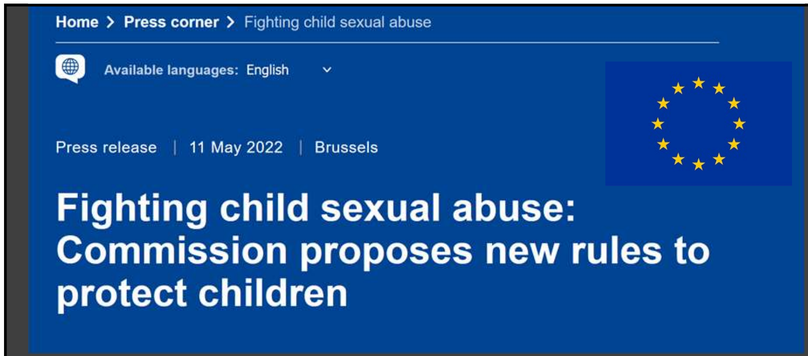
International Statement: End-To-End Encryption and Public Safety

- 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 […]

The CSAM story (Child Abuse Sexual Material)

- Driven by NCMEC (US)
- Detects CSAM content
  - PhotoDNA: secret perceptual hash function
  - secret list of hash values of content
- Many 100K detections per year
- Threatened by end-to-end encryption


1
2
672491352812...
3
672491352812...
4
5
PhotoDNA™
The Next Chapter in Protecting Children Online
MICROSOFT DIGITAL CRIMES UNIT
facebook
Microsoft



Home > Press corner > Fighting child sexual abuse

Available languages: English

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
- Client side scanning for known content
- Detect grooming using AI

Threshold private set intersection (PSI) with associated data (tPSI-AD) [August 2021]

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 only 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.

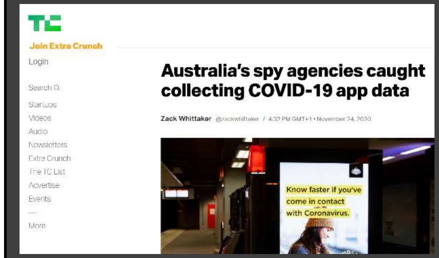
July 29, 2021

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.

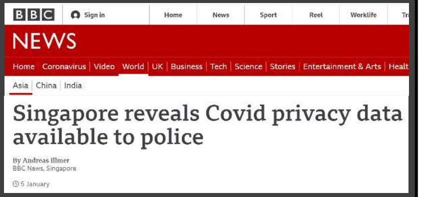
- Needs perceptual hash function: NeuralHash (96 bits)

Problem 1: Mission Creep



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

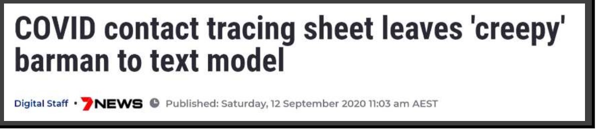
Zack Whittaker @zackwhittaker / 4:32 PM GMT+1 • November 24, 2020



Singapore reveals Covid privacy data available to police

By Andreas Illmer
BBC News, Singapore

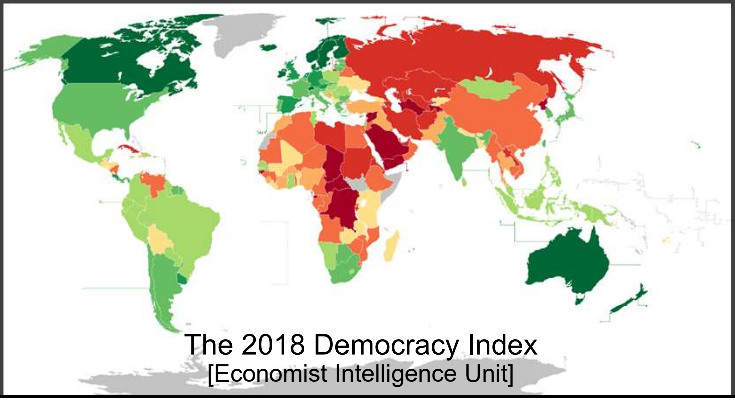
5 January



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

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

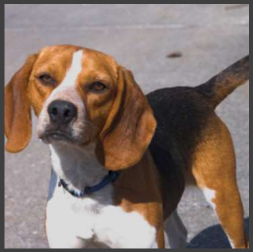
Problem 2: Unauthorized Surveillance

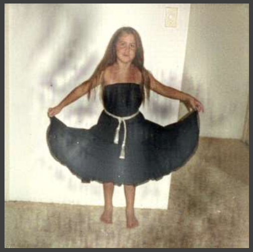


The 2018 Democracy Index
[Economist Intelligence Unit]

Problem 3: Framing

through NeuralHash collisions
https://blog.roboflow.com/neuralhash-collision/





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

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

Problem 4: Correctly detecting grooming in written and spoken language is likely well beyond the state of the art

Are there other options for law enforcement?

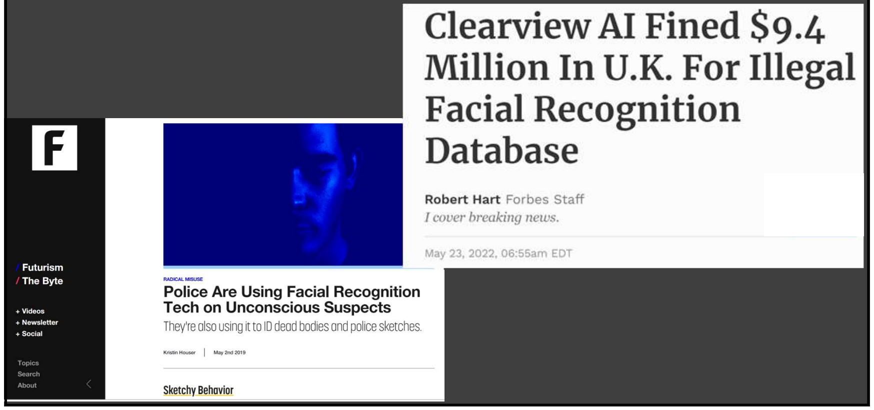
Options for Law Enforcement (2/4)

- **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**

metadata

Law enforcement: metadata is insufficient

AI?



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

RADICAL MISUSE

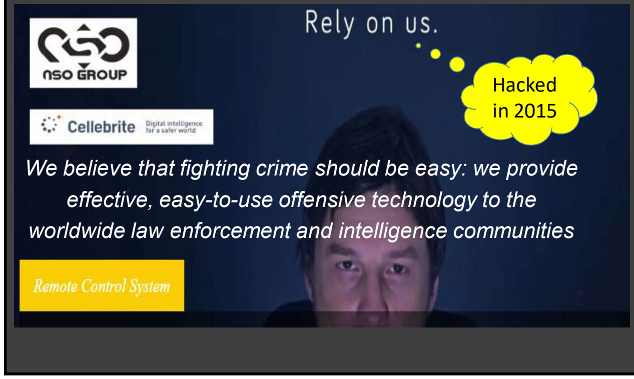
Police Are Using Facial Recognition Tech on Unconscious Suspects

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

Kristin Houser | May 2nd 2019

Sketchy Behavior

Options for Law Enforcement (3/4)

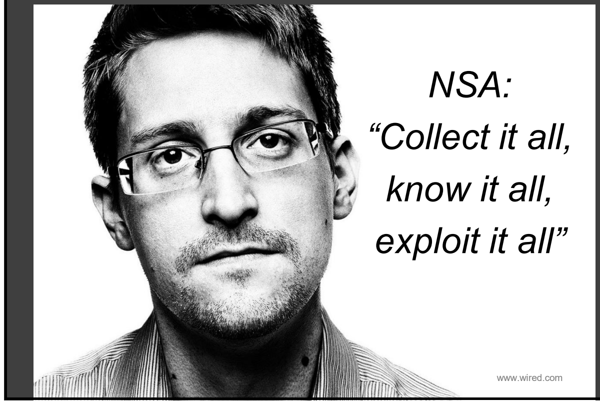


We believe that fighting crime should be easy: we provide effective, easy-to-use offensive technology to the worldwide law enforcement and intelligence communities

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

DE: Bundestrojaner: key logger, screenshots, Skype calls

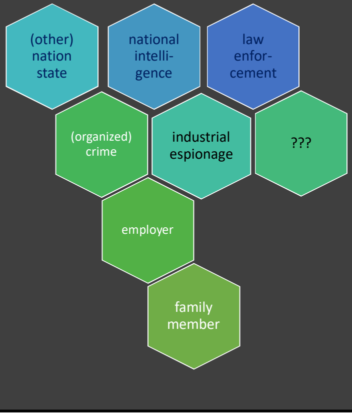
Options for Law Enforcement (4/4)



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

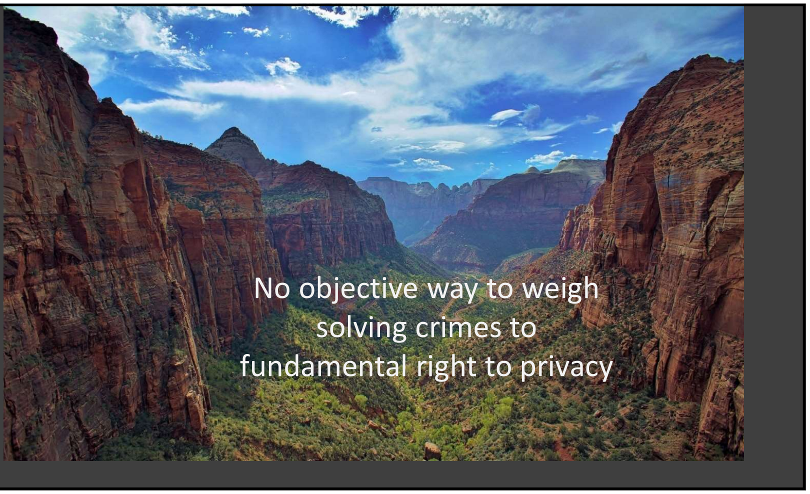
Collaborate with intelligence services

The bigger picture



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



No objective way to weigh solving crimes to fundamental right to privacy

But who shall watch over the (cyber) guards?

Conclusions: policy

Crypto wars ongoing

- limited support for key escrow/backdoors
- backdoors are now imposed in more countries (UK/Australia)
- CSAM may be game changer (policy wise)
- hacking by police is much more risky

- Main problem is still building secure systems for citizens
- Need open debate with all elements on the table

Conclusions: research

Research needed on future options

- risks: don’t make the current insecurity worse
- accountability
- transparency

Researchers need to engage in public policy

Bart Preneel

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

53