

Cybersecurity policy: the never-ending crypto wars

KU LEUVEN



nextAuth

Best in mobile user authentication

COSIC



Bart Preneel

COSIC, KU Leuven

@bpreneel1

preneel@infosec.exchange

Amusec - 25 May 2023

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

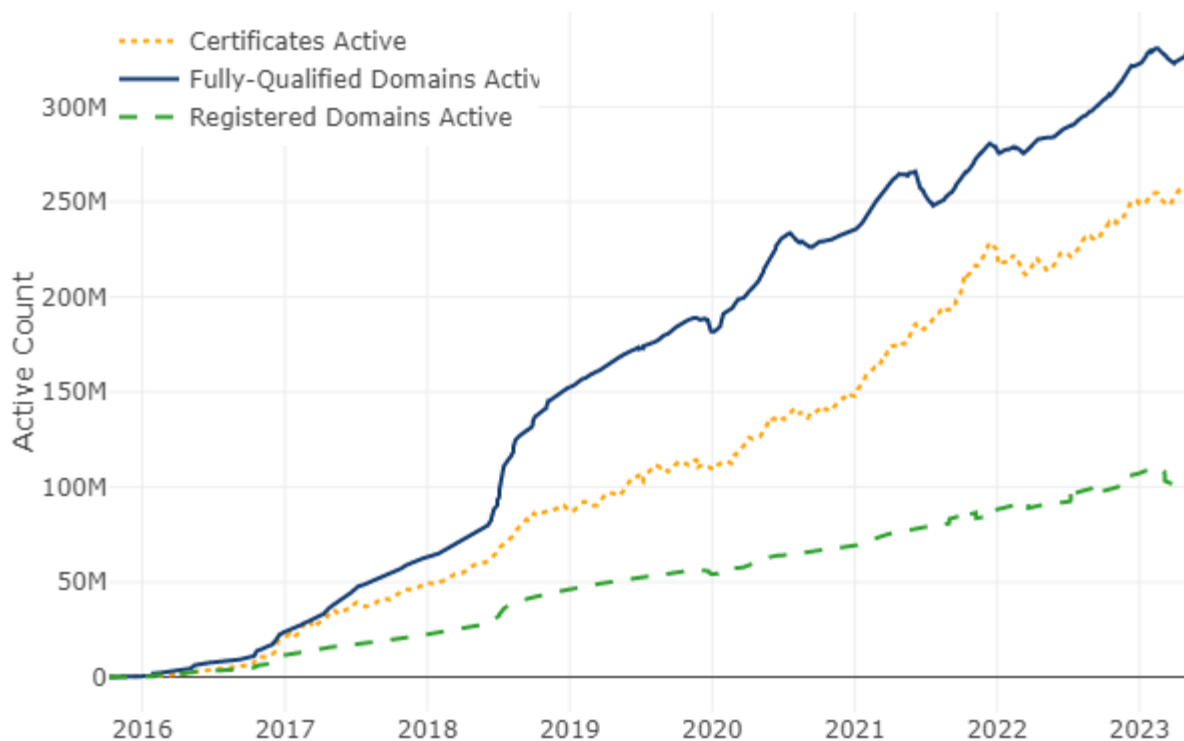


Free certs - live since November 2015

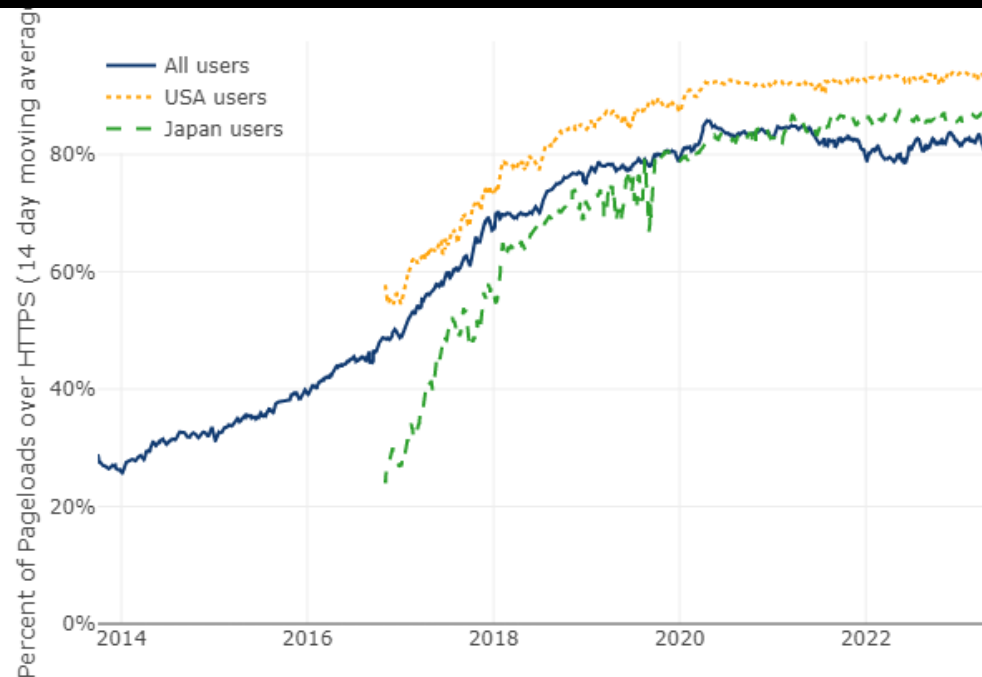
260 M active certificates

<https://letsencrypt.org/>

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.

SINK CLIPPER!



Because some things
are better left unread.



Crypto Museum
cryptomuseum.com

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.*

A photograph of David Cameron, the former Prime Minister of the United Kingdom, speaking at a public event. He is wearing a dark suit, a white shirt, and a blue tie. He is gesturing with his right hand, pointing towards the right side of the frame. The background is blurred, showing a large Union Jack flag.

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

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





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)



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

SECTION SUPPORTERS



ADVERTISING

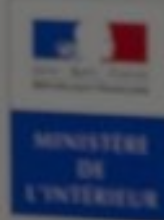
FOR A BETTER
CONNECTED EUROPE

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

A photograph of two men in suits standing at a press conference. The man on the left is looking down at a blue folder he is holding. The man on the right is looking towards the camera. Behind them are the German, European Union, and French flags. The scene is set against a blue background.

France and Germany push for encryption limits (2016)

ieur



Ministère de l'I

23 août 201



$$e^{i\pi} = 999$$

*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



Chip Somodevilla/Getty Images

“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 conference in Boston this month, referring to encryption that thwarts investigators. [F.B.I. Director](#)

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

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

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

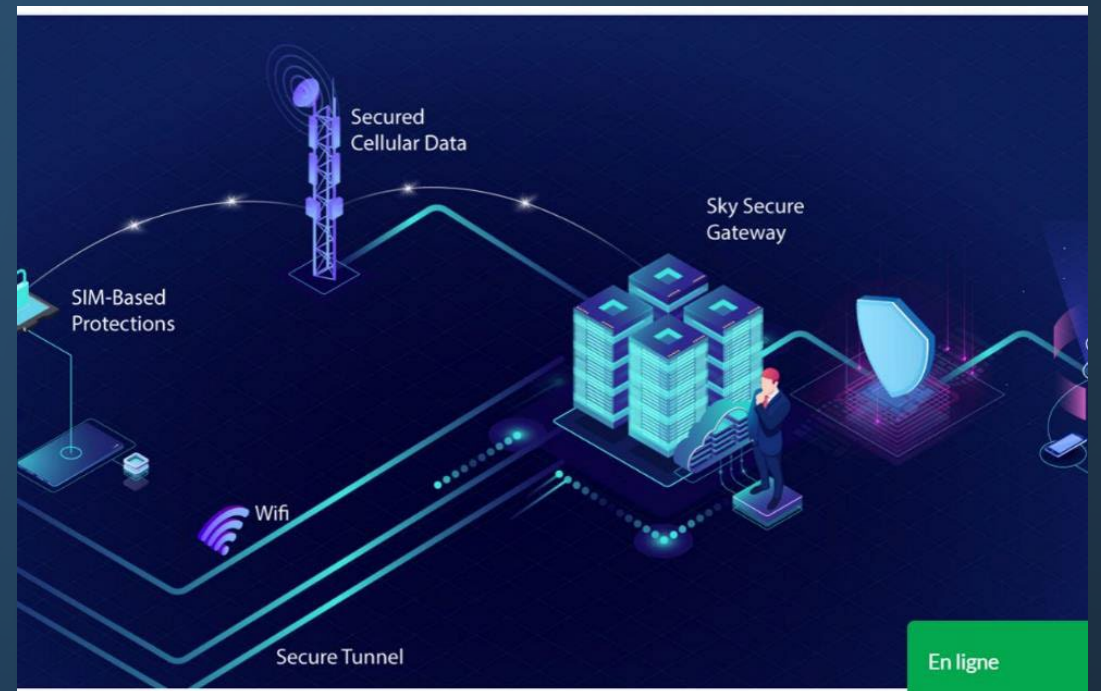
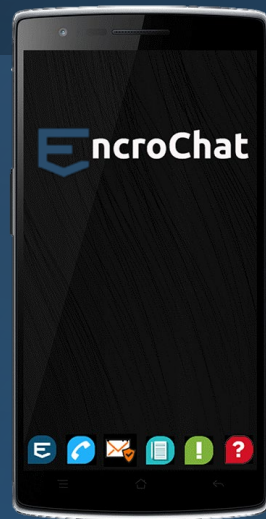
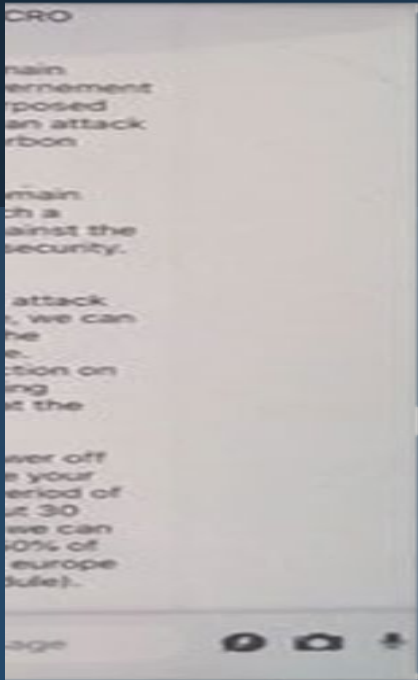
National Security

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)

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

Can cryptography solve the problem
created by cryptography?



FBI Director Christopher Wray

[2018] We can find solutions to the Going Dark problem.

...

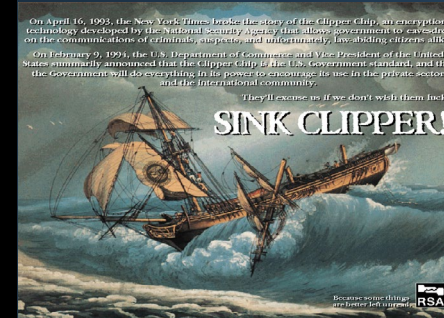
If we can develop driverless cars ... surely we should be able to design devices that both provide data security and permit lawful access with a court order.

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



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



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

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.

Problem 1: Mission Creep

TC
Join Extra Crunch

Login

Search Q

StarLups

Videos

Audio

Newsletters

Extra Crunch

The TC List

Advertise

Events

—

More

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

Zack Whittaker @zackwhittaker / 4:52 PM GMT+1 • November 24, 2020



Singapore reveals Covid privacy data available to police

By Andreas Illmer
BBC News, Singapore

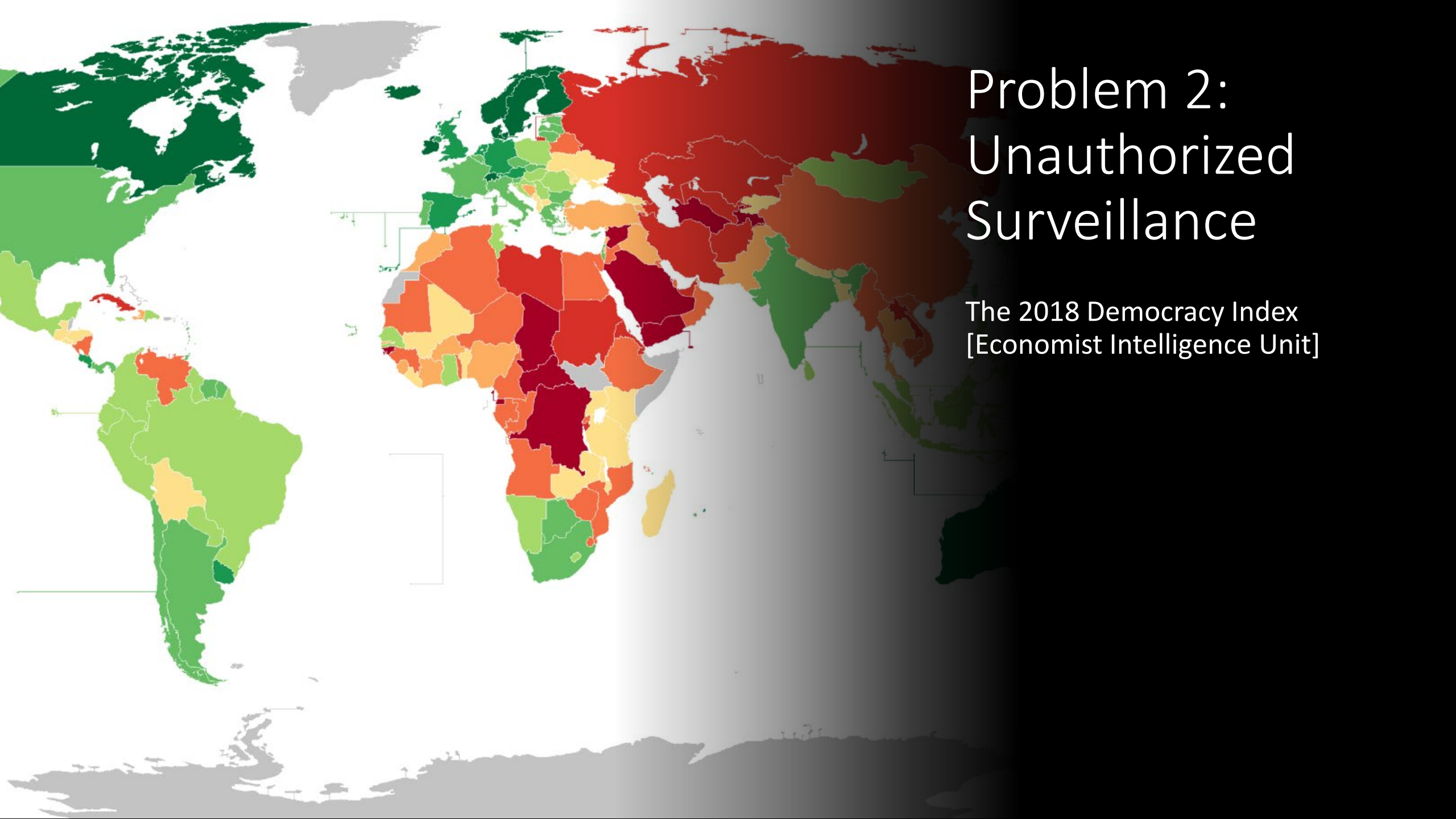
© 5 January

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

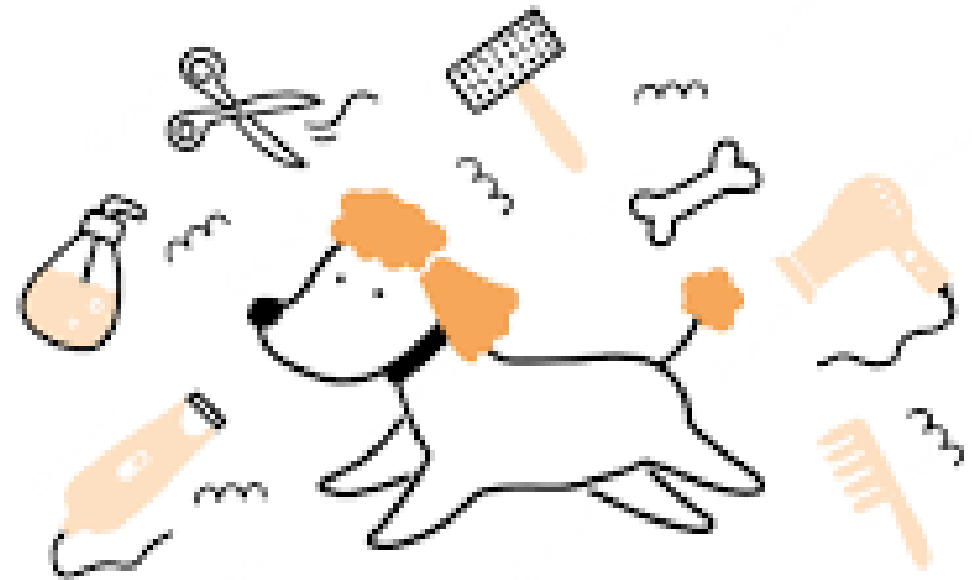
<https://blog.roboflow.com/neuralhash-collision/>



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



PET
Grooming

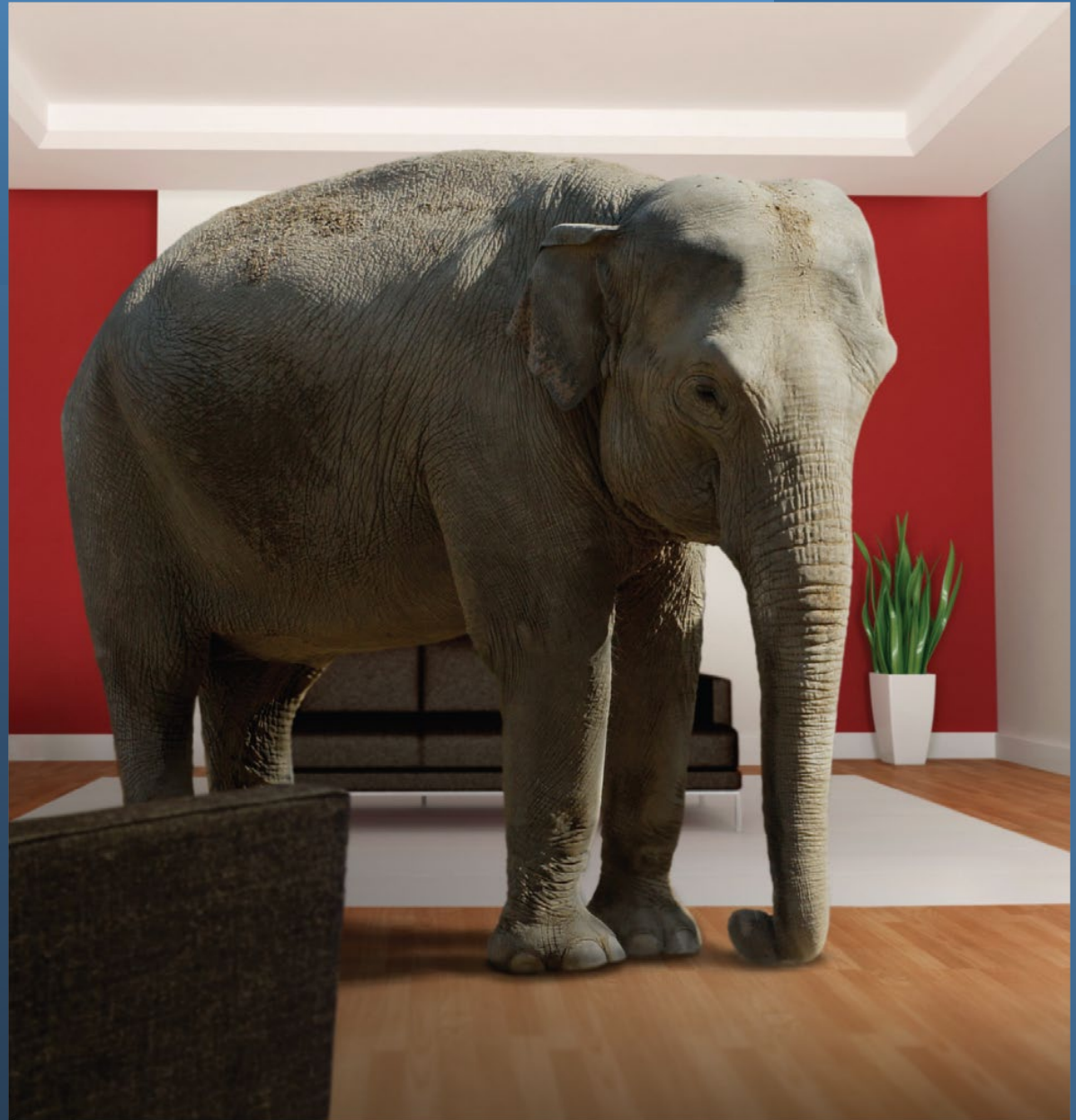
Are there other options
for law enforcement?

Options for Law Enforcement (2/4)

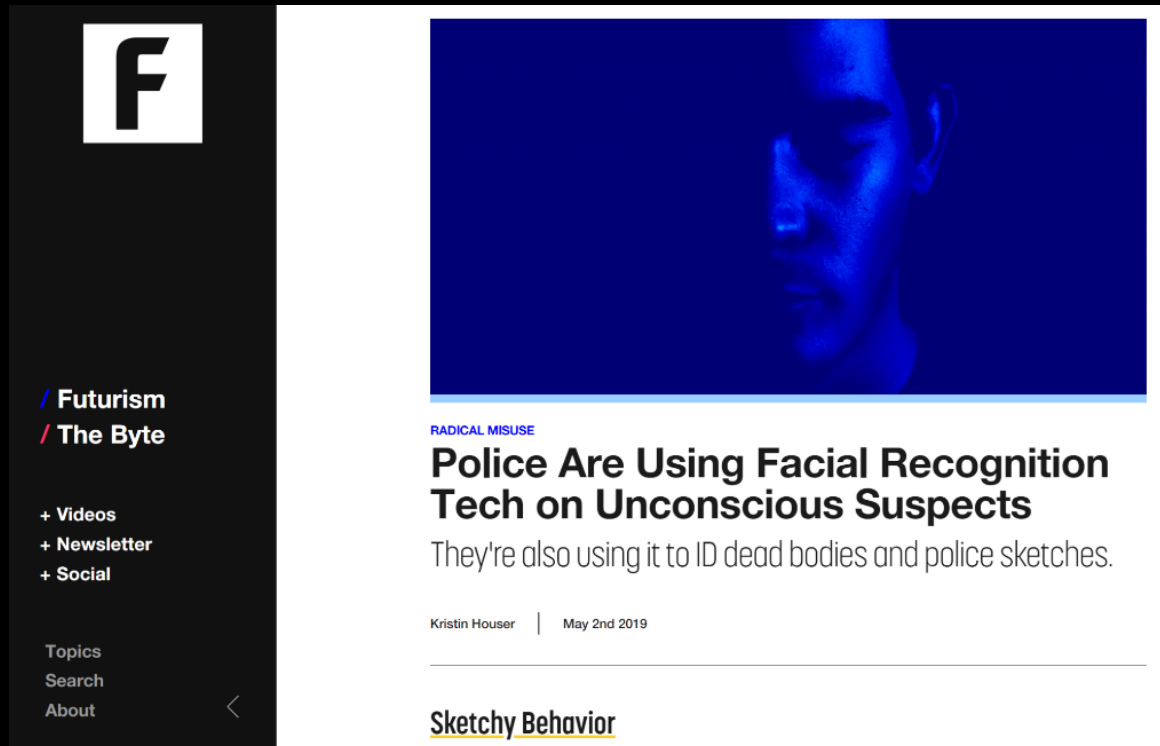
- **exploit operational security weaknesses:** operating a system securely is difficult
 - e.g. password cracking
- obtain **technical assistance from industry** to bypass decryption or to access keys
 - remote update
 - backup in cloud
 - iPhone unlock from Cellebrite or Grayshift
- **use metadata**
- **use AI**

metadata

Law enforcement:
metadata is
insufficient



AI?




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

Options for Law Enforcement (3/4)



Rely on us.

Hacked
in 2015

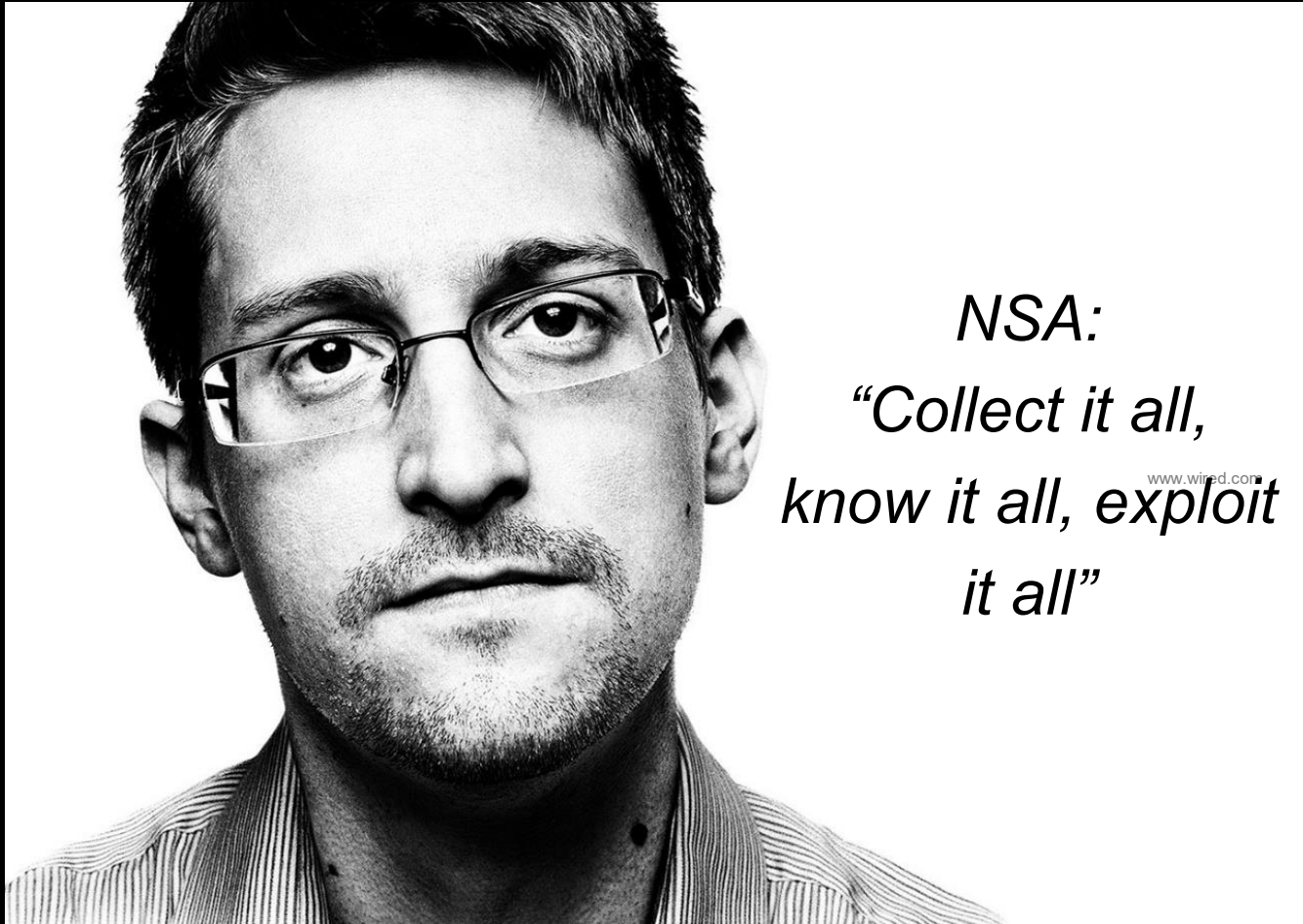
We believe that fighting crime should be easy: we provide effective, easy-to-use offensive technology to the worldwide law enforcement and intelligence communities

Remote Control System

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

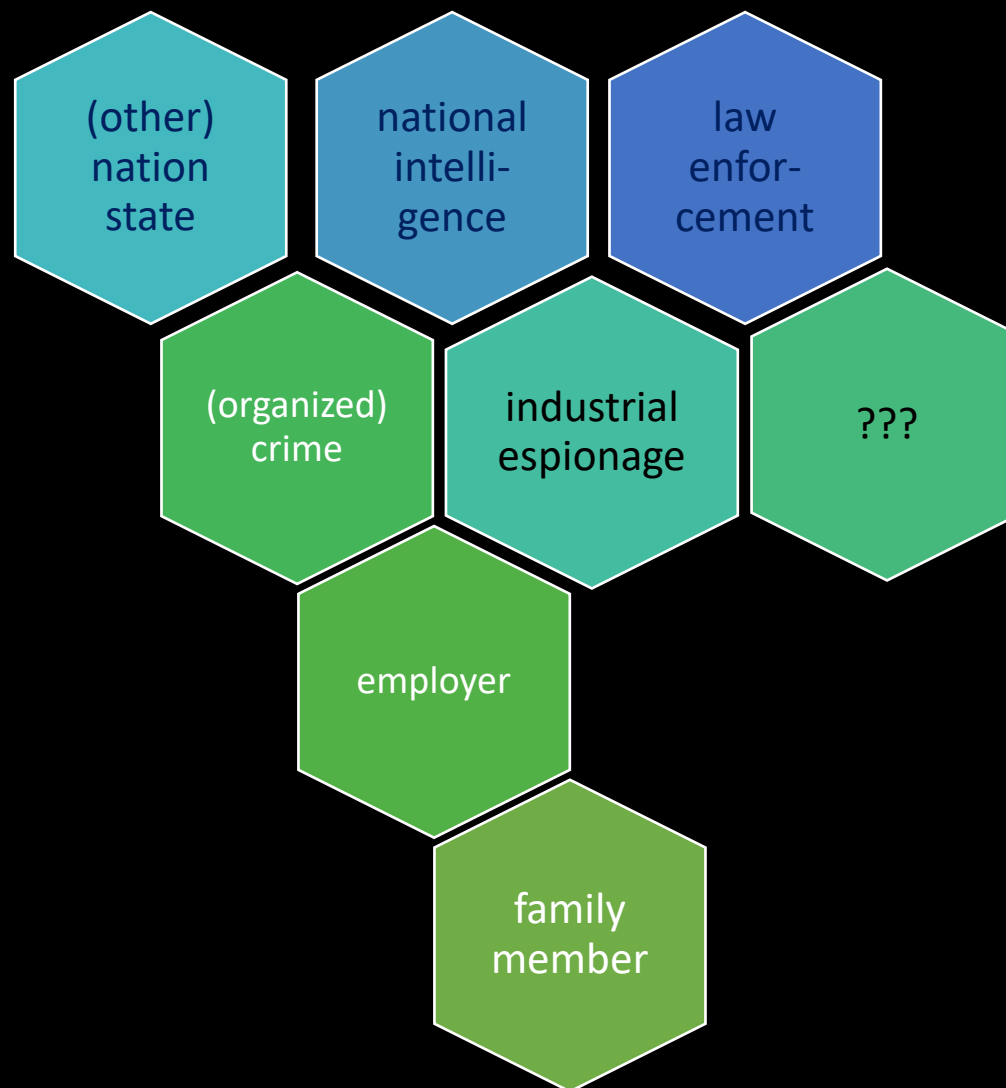
DE:
Bundestrojaner:
key logger,
screenshots,
Skype calls

Options for Law Enforcement (4/4)



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

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

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

TELEPHONE: +32 16 321148

KU LEUVEN

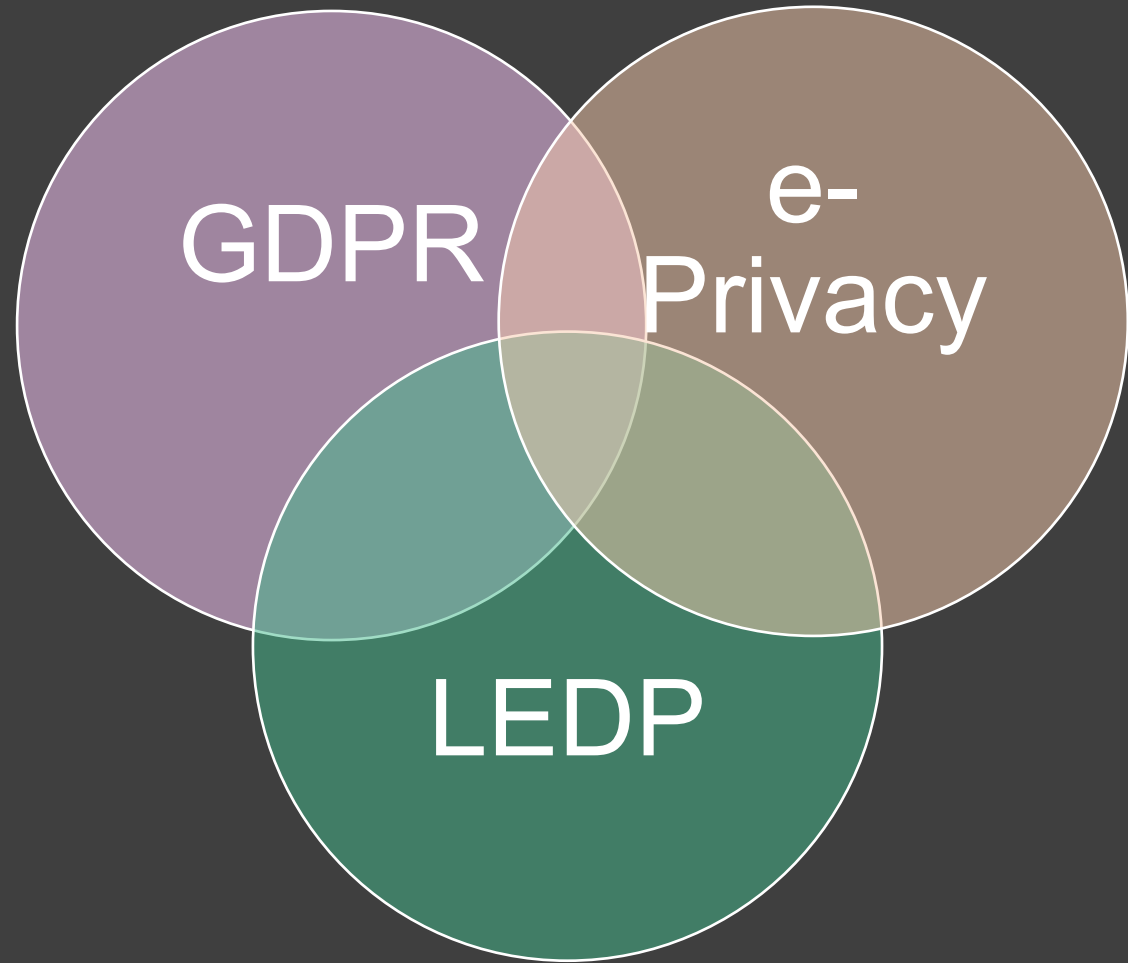


nextAuth
Best in mobile user authentication

COSIC



Legal



GDPR Art 23

• Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

- (a) national security;
- (b) defence;
- (c) public security;
- (d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
- (e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;
- (f) the protection of judicial independence and judicial proceedings;
- (g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
- (h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);
- (i) the protection of the data subject or the rights and freedoms of others;
- (j) the enforcement of civil law claims.

E-Privacy Regulation (ePR)

- electronic communications services such as WhatsApp, Facebook Messenger and Skype. ensure that these popular services guarantee the **same level of confidentiality** of communications as traditional telecoms operators
- privacy is guaranteed for communications **content and metadata**. Metadata have a high privacy component and is to be anonymised or deleted if users did not give their consent, unless the data is needed for billing.
- Any interference with the content of electronic communications should be allowed only under very clear defined conditions, for specific purposes and be subject to adequate safeguards against abuse.
 - further processing for compatible purposes:
 - e.g. tracking of mobile phones for applications -> voluntary data retention?
 - tracking walls
 - national security or defence excluded from the scope: quid case law of the CJEU on data retention?
 - Consequence: GDPR Article 23 or outside scope of EU law

Directive for Law enforcement agencies (LEDP)

- Unclear relation to activities of **intelligence agencies that fall outside of EU legal competence**, but where the EU itself, for example through Europol, is increasing its activities
- Unclear consequences for the **data gathered pro-actively and/or in bulk** on people who are **not** linked to any criminal activity, contrary to the protection of fair trial rights in Art. 6 ECHR and Art. 47 of the Charter of Fundamental Rights of the European Union.
- Current articles on lawful processing (7 and 7a) **could allow massive transfer of data** from law enforcement agencies in the Member States (inside the Directive's scope) to the respective **national security agencies** (outside the Directive's scope).