DS 593: Privacy in Practice

Frontiers of Privacy

Instructor: Alishah Chator

News?

CDS DS 593 A1 - Special Topics in Data Science Methodologies

Student

https://go.blueja.io/atVxKqkBWECR5alJXV2EZw

To access the evaluation, scan this QR code with your mobile phone.

Why try?

There is a lot to be discouraged about

- Data extractive practices everywhere
- So much of our data is already exposed
- A messy legal landscape
- Have to pick between panopticon or chaos
- Powerful spyware and state actors
- A feeling like perfect privacy is unachievable

So what hope is there?

Concern: They already have my data

Concern: They already have my data

- We are dynamic: there will always be more data out there to save
- Having data == power, but power always shifts around
- Everything has to start somewhere
- Having data is not necessarily the same thing as being able to use that data

Concern: No Concrete Privacy Protections

Concern: No Concrete Privacy Protections

- We have made huge strides in conceptualizing and understanding what it means to protect privacy
  - Its not just about hiding data!
  - Harms-centered approach
- We have a much clearer sense of what aspects we try to solve with technology and which parts need regulation
- By not just focusing on “Data Hiding” we can avoid some of this defeatism
  - However, just on the point of ”data hiding” we already have some wins!

Concern: Pegasus

Concern: Pegasus

- This is a bit of a tough one

Concern: Pegasus

- This is a bit of a tough one

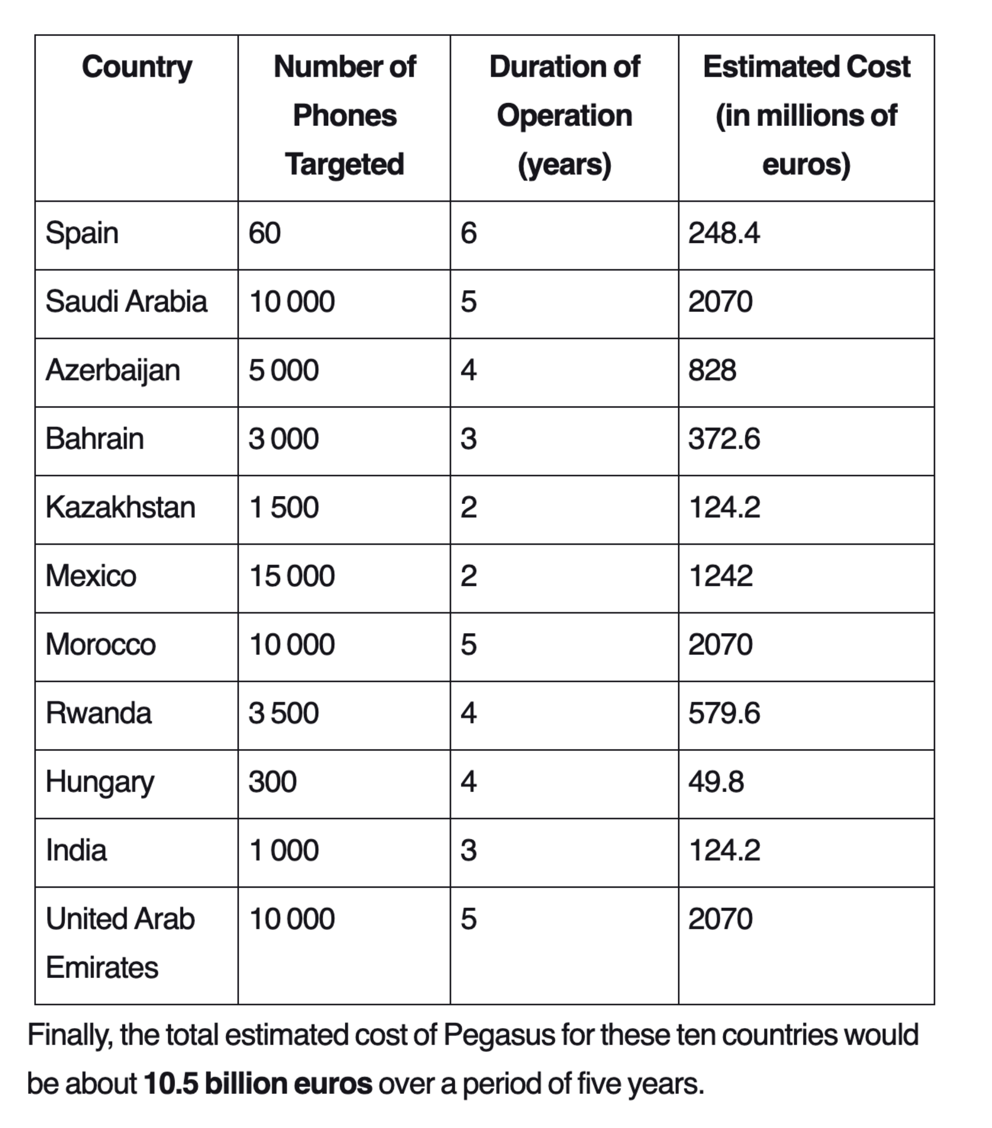
- True statement: It is very unlikely your privacy protections will hold up against an extremely resourced adversary who is determined to go after you

Concern: Pegasus

- This is a bit of a tough one

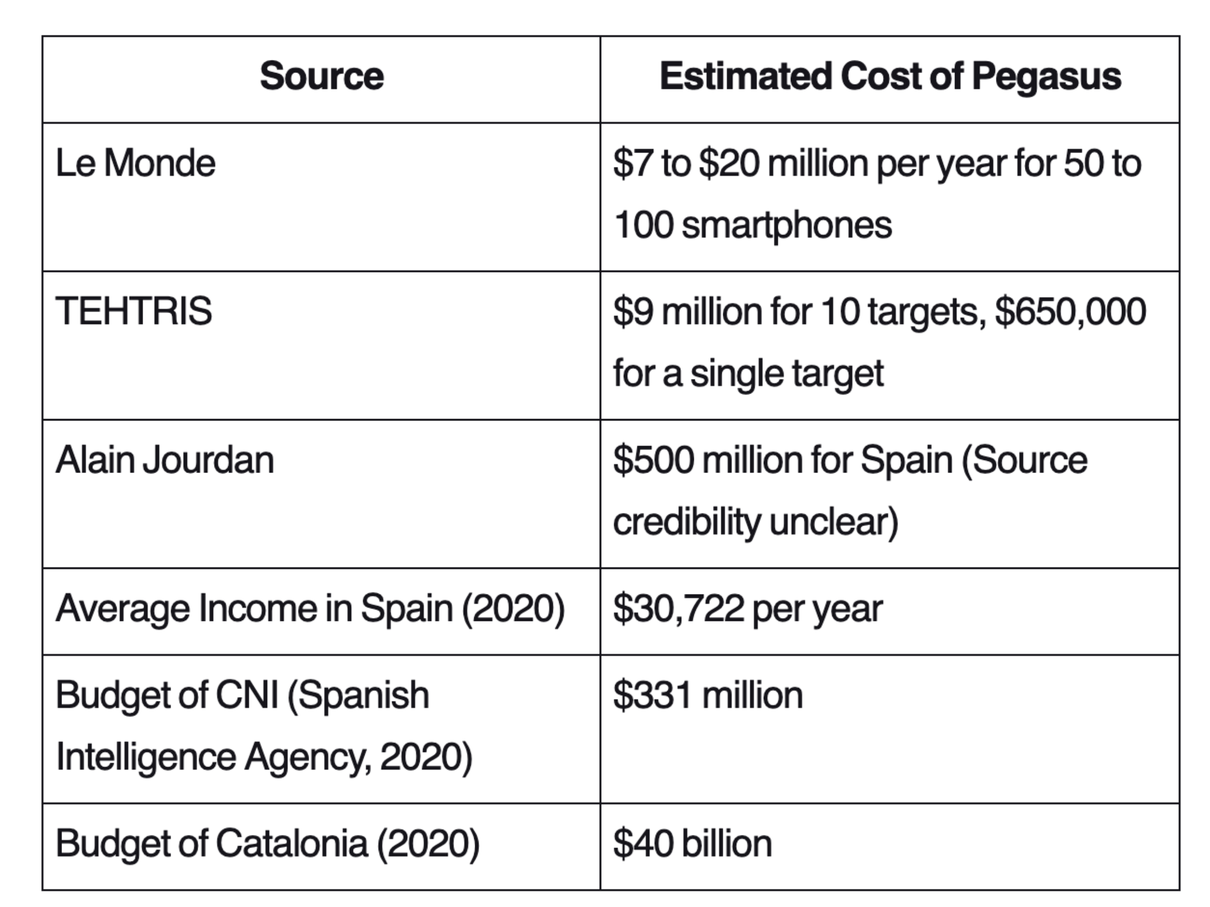
- True statement: It is very unlikely your privacy protections will hold up against an extremely resourced adversary who is determined to go after you

- But this isn’t cheap
  - Mass vs targeted surveillance
  - The NSA vs the ICE officer vs a Cop



Country	Number of Phones Targeted	Duration of Operation (years)	Estimated Cost (in millions of euros)
Spain	60	6	248.4
Saudi Arabia	10 000	5	2070
Azerbaijan	5 000	4	828
Bahrain	3 000	3	372.6
Kazakhstan	1 500	2	124.2
Mexico	15 000	2	1242
Morocco	10 000	5	2070
Rwanda	3 500	4	579.6
Hungary	300	4	49.8
India	1 000	3	124.2
United Arab Emirates	10 000	5	2070

Finally, the total estimated cost of Pegasus for these ten countries would be about **10.5 billion euros** over a period of five years.

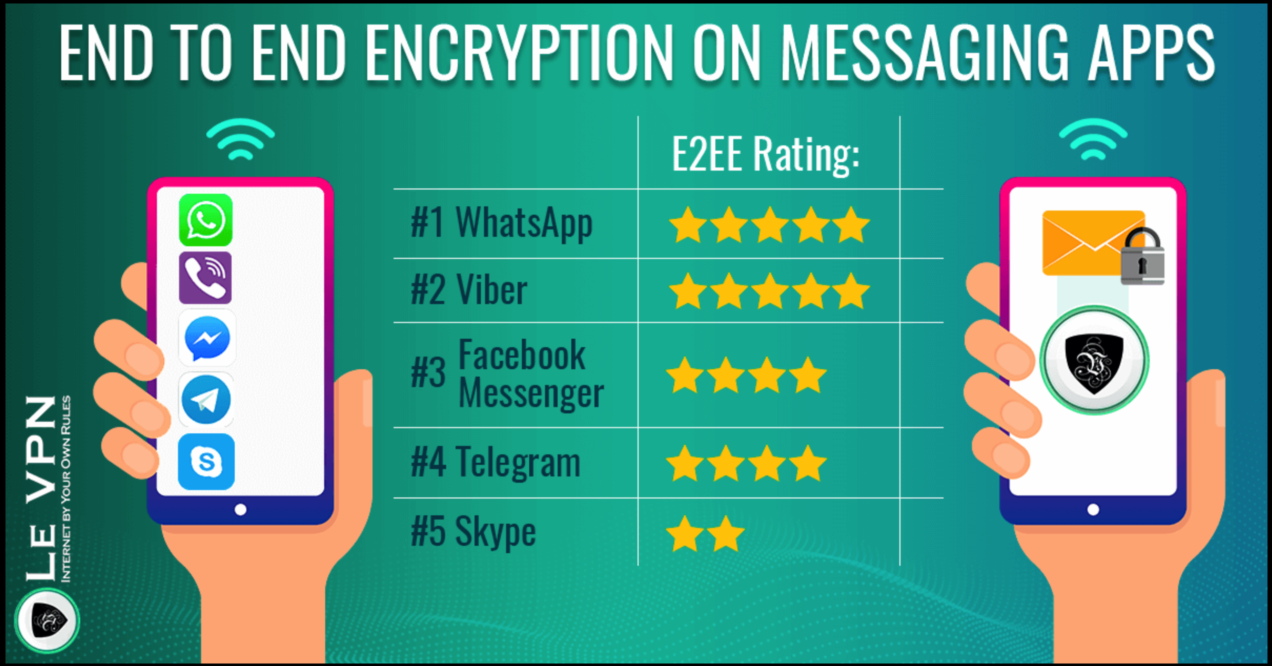


Source	Estimated Cost of Pegasus
Le Monde	$7 to $20 million per year for 50 to 100 smartphones
TEHTRIS	$9 million for 10 targets, $650,000 for a single target
Alain Jourdan	$500 million for Spain (Source credibility unclear)
Average Income in Spain (2020)	$30,722 per year
Budget of CNI (Spanish Intelligence Agency, 2020)	$331 million
Budget of Catalonia (2020)	$40 billion

https://freemindtronic.com/pegasus-the-cost-of-spying-with-one-of-the-most-powerful-spyware-in-the-world/

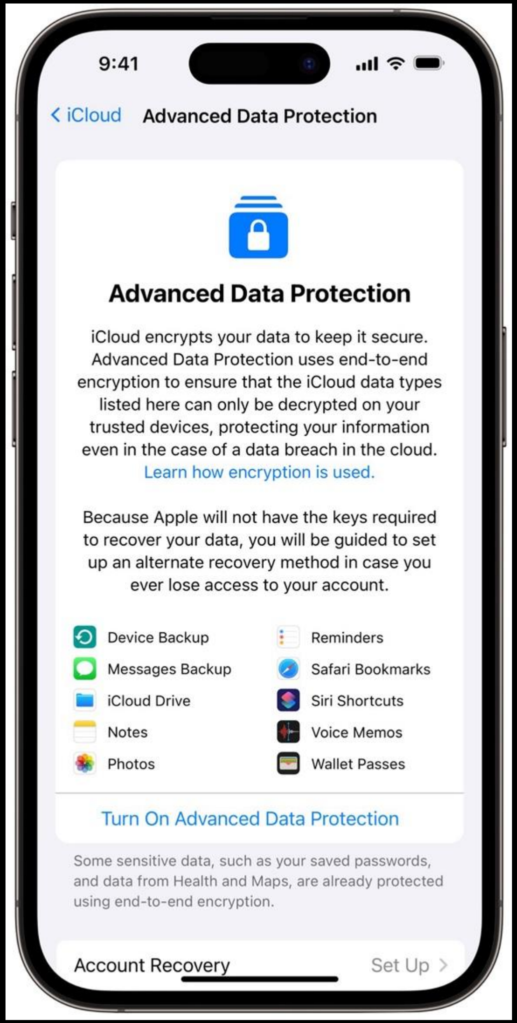
We may not be able to stop all of it but we can at least make it costly!

Things that give me hope



END TO END ENCRYPTION ON MESSAGING APPS

	E2EE Rating:
#1 WhatsApp	★★★★★
#2 Viber	★★★★★
#3 Facebook Messenger	★★★★
#4 Telegram	★★★★
#5 Skype	★★



Advanced Data Protection

Advanced Data Protection

iCloud encrypts your data to keep it secure. Advanced Data Protection uses end-to-end encryption to ensure that the iCloud data types listed here can only be decrypted on your trusted devices, protecting your information even in the case of a data breach in the cloud. Learn how encryption is used.

Because Apple will not have the keys required to recover your data, you will be guided to set up an alternate recovery method in case you ever lose access to your account.

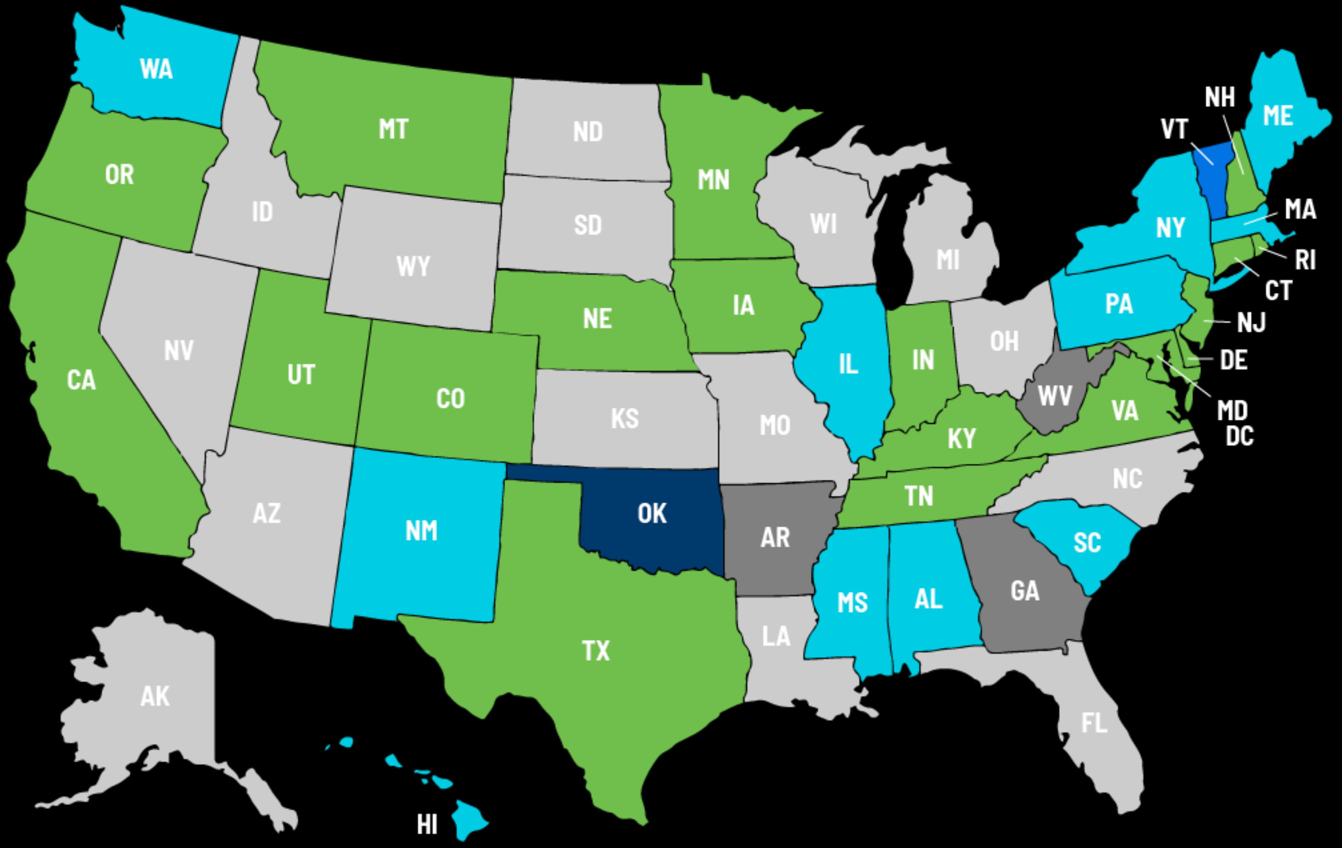
- Device Backup
- Messages Backup
- iCloud Drive
- Notes
- Photos
- Reminders
- Safari Bookmarks
- Siri Shortcuts
- Voice Memos
- Wallet Passes

Some sensitive data, such as your saved passwords, and data from Health and Maps, are already protected using end-to-end encryption.

Account Recovery: Set Up >

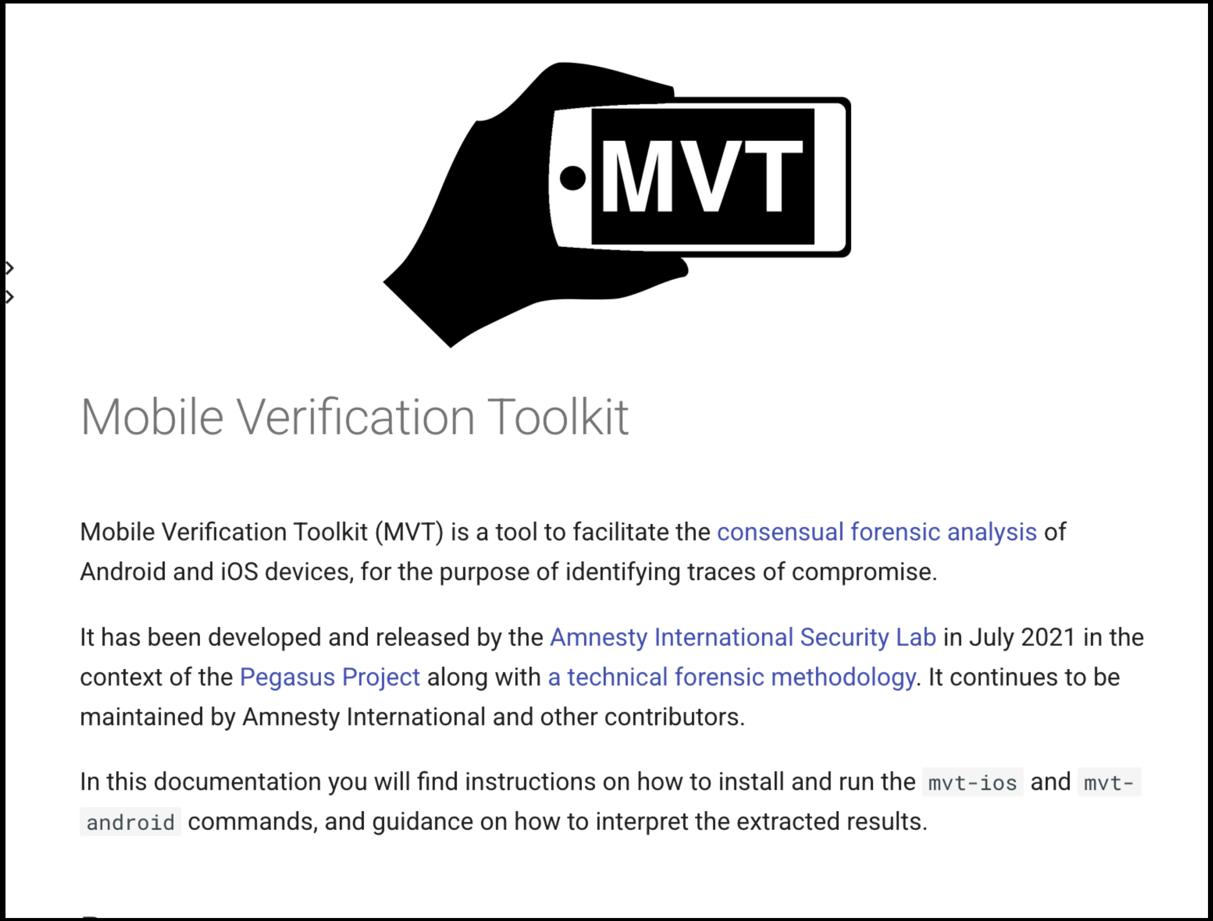
iapp

US State Privacy Legislation Tracker 2025



Statute/bill in legislative process:

- 🟨 Introduced
- 🟦 In committee
- 🟦 In cross chamber
- ⬛ In cross committee
- 🟩 Passed
- 🟩 Signed
- ⬛ Inactive bills
- ⬜ No comprehensive bills introduced
- ⟳ Last updated 21 Apr. 2025

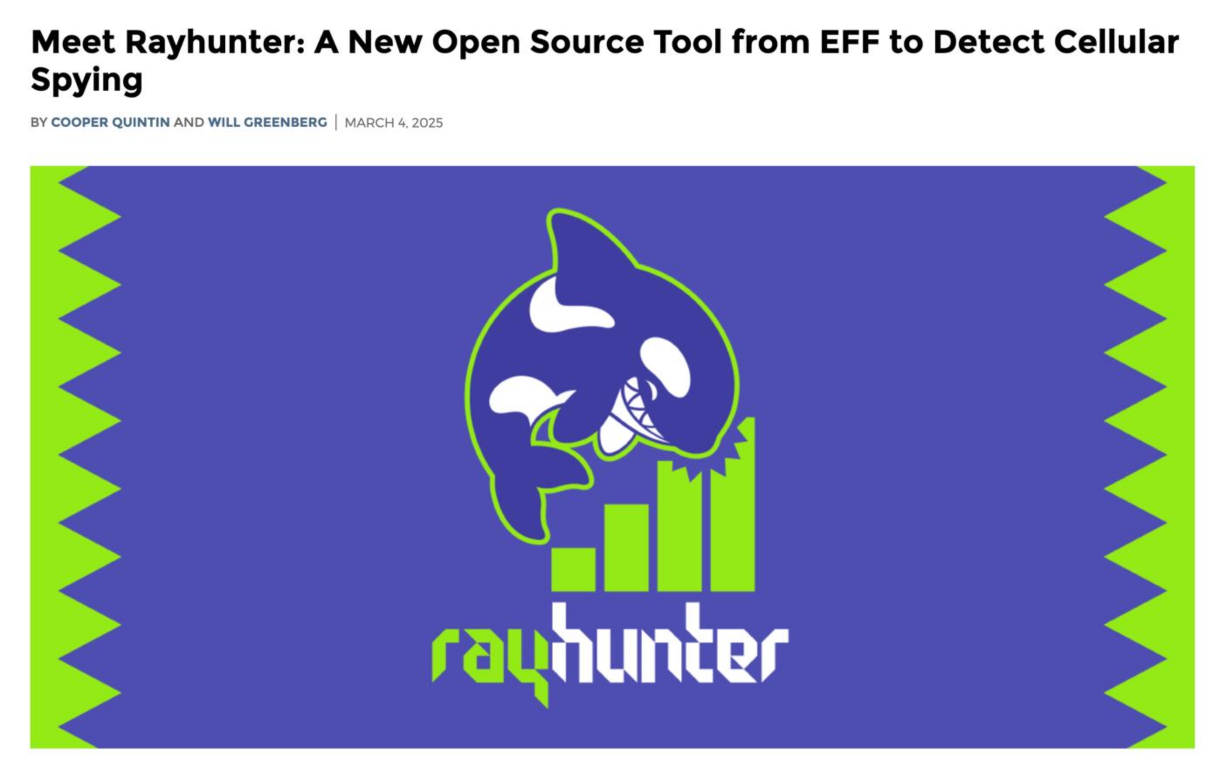


Mobile Verification Toolkit

Mobile Verification Toolkit (MVT) is a tool to facilitate the consensual forensic analysis of Android and iOS devices, for the purpose of identifying traces of compromise.

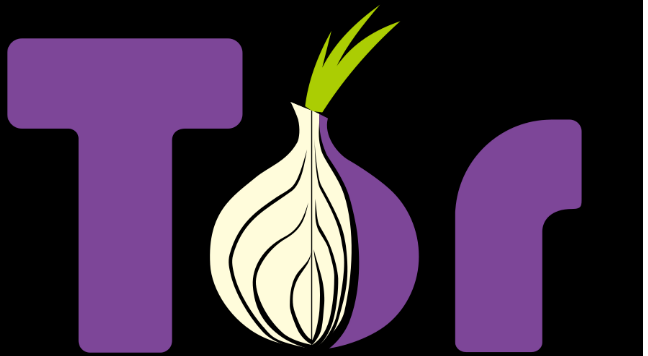
It has been developed and released by the Amnesty International Security Lab in July 2021 in the context of the Pegasus Project along with a technical forensic methodology. It continues to be maintained by Amnesty International and other contributors.

In this documentation you will find instructions on how to install and run the `mvt-ios` and `mvt-android` commands, and guidance on how to interpret the extracted results.

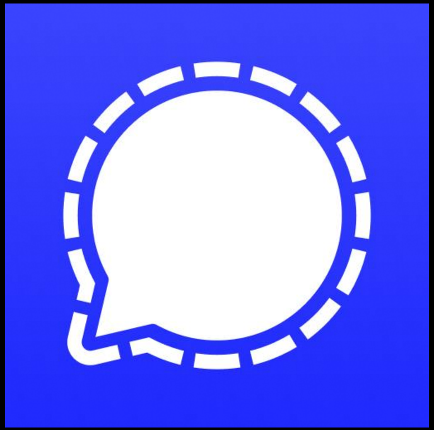


Meet Rayhunter: A New Open Source Tool from EFF to Detect Cellular Spying

BY COOPER QUINTIN AND WILL GREENBERG | MARCH 4, 2025

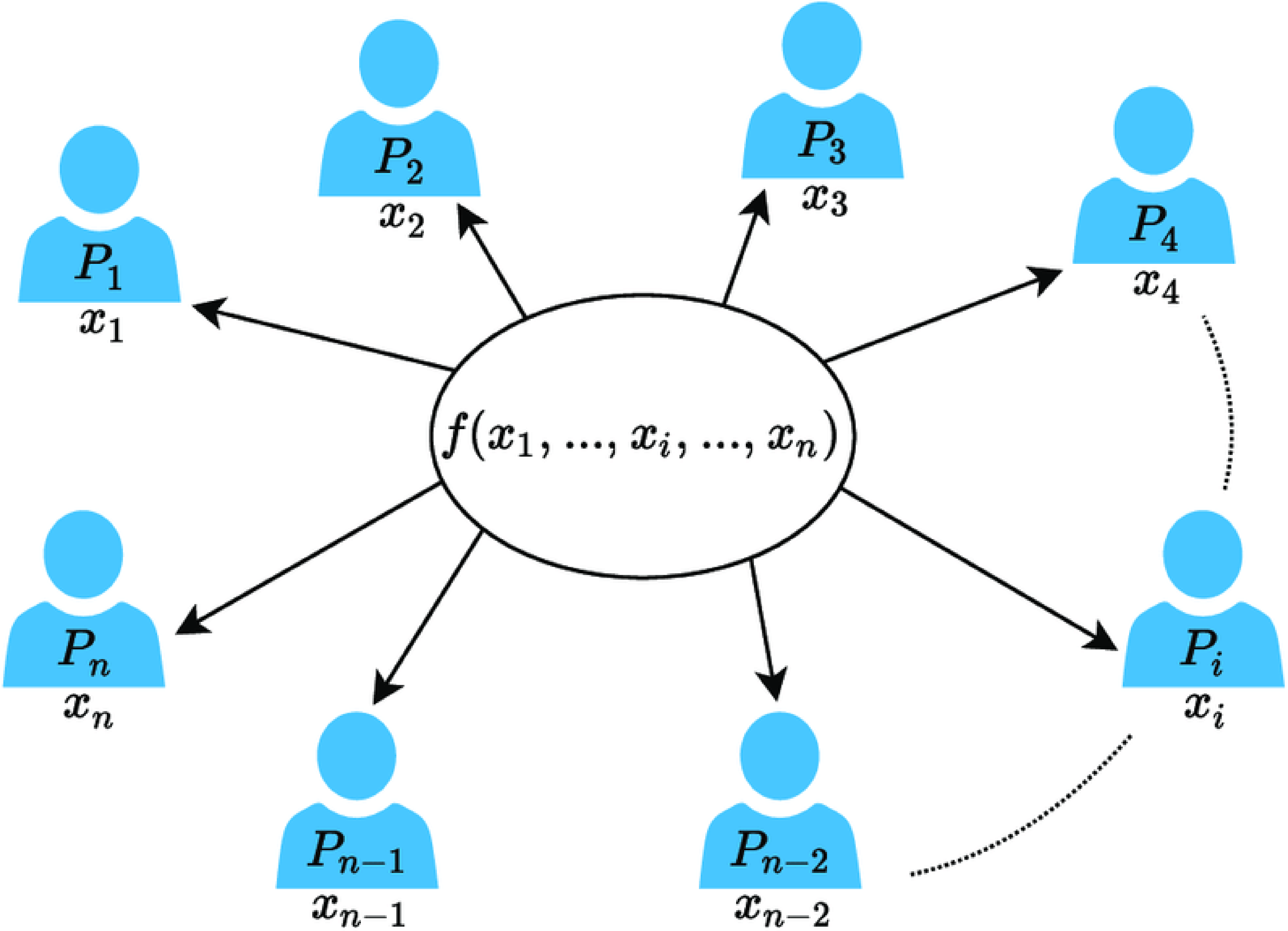

Tor

CryptPad



Tails
theamnesicincognitolivesystem

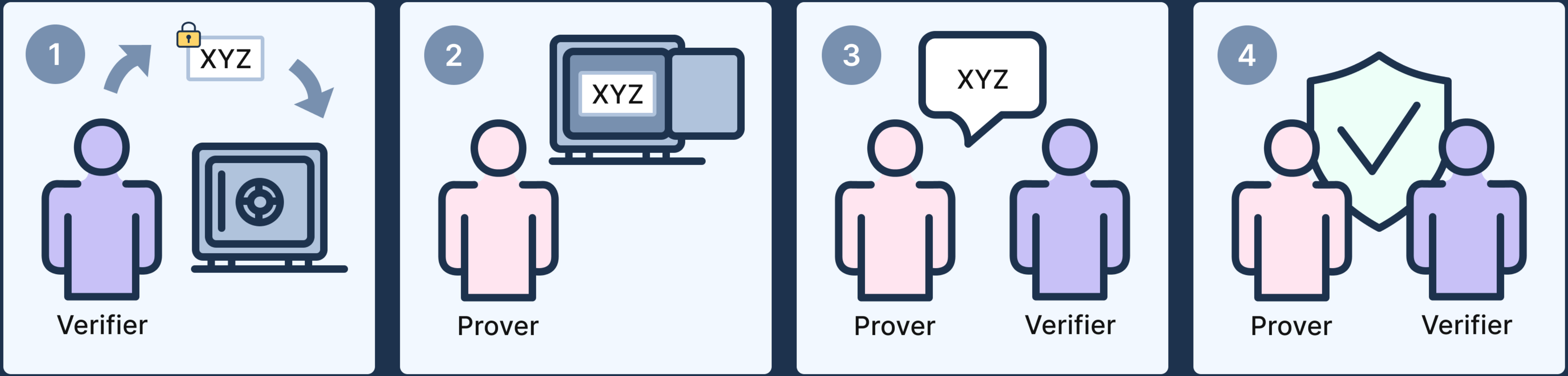
bitwarden


P_1
x_1
P_2
x_2
P_3
x_3
P_4
x_4
$f(x_1, ..., x_i, ..., x_n)$
P_n
x_n
P_i
x_i
P_{n-1}
x_{n-1}
P_{n-2}
x_{n-2}

How a zero-knowledge proof works

CIRCULARISE

Prove that you know the combination code to a safe without revealing the code



1. Verifier writes a secret message and put it in a locked safe.

2. Prover who fulfils the requirements has knowledge of the combination code and opens the locked safe.

3. Prover returns the secret message to Verifier.

4. Verifier is convinced that the prover knows the combination and can be trusted.

June 10, 2024

Private Cloud Compute: A new frontier for AI privacy in the cloud

Written by Apple Security Engineering and Architecture (SEAR), User Privacy, Core Operating Systems (Core OS), Services Engineering (ASE), and Machine Learning and AI (AIML)

Thank you!