TousAntiCovid

The French Contact Tracing Apps

Claude Castelluccia, Privatics Inria

Disclaimer: my own view, not from Inria or FR gov.

From StopCovid to TousAntiCovid

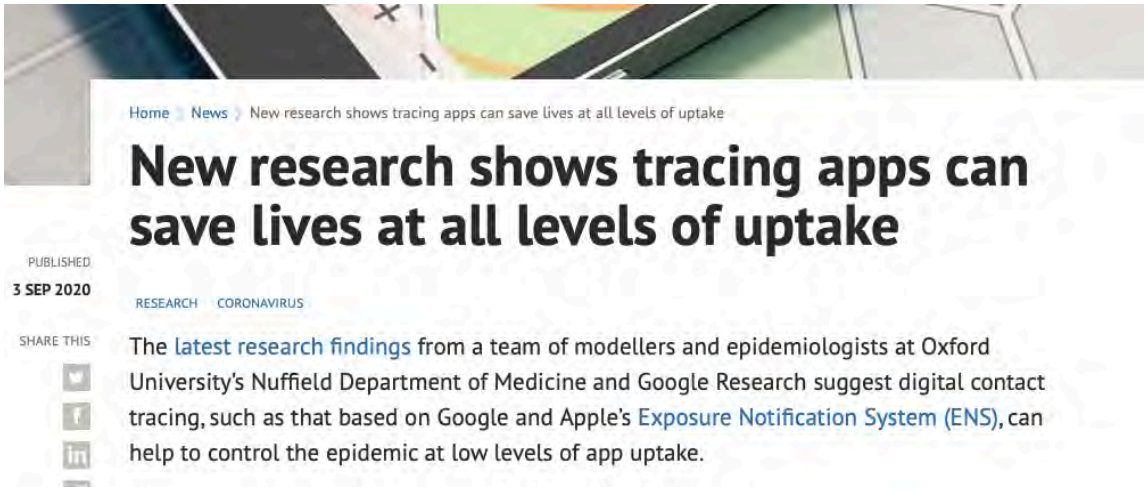
- Work started in mid-march as an “Inria” internal project
- Design constraints
  - System must be controled/managed by Health authority
  - System must be Privacy-Preserving and GDPR compliant
- First version was “decentralized” (discussions with DP3T)
  - But soon we realized that this will not work (both constraints not satisfied!)
- End of march, we moved to a so-called “centralized” approach and teamed-up with German CT team (who was about to launch their system!).
- We launch *StopCovid* in June
- A new version, *TousAntiCovid*, was released in October

TousAntiCovid

- *TousAntiCovid* includes 3 (soon 4) functionalities
  - Contact Tracing (based on ROBERT)
  - News kiosk (information about Covid and TousAntiCovid)
  - Attestations (necessary to move during lock down)
- About 10,5 millions registered users as of today

Digital Contact Tracing

- **Complementary** to manual contact tracing
- Most digital tools (at least in EU) do no trace contacts, but:
  - Compute an **exposure score** from contacts…
  - Notify users (but **don't trace** them)!
    - For example a user is notify if exposed more than 15min at less than 1.5 meters (moved to 5min and 2m recently).
    - It could be 15 min with one infected persons or few minutes with several infected persons!
    - Notified users won't learn the infected sources (at least should not)
- A tool to help public health authorities, **not standalone one**…



Home › News › New research shows tracing apps can save lives at all levels of uptake

New research shows tracing apps can save lives at all levels of uptake

PUBLISHED
3 SEP 2020

RESEARCH CORONAVIRUS

SHARE THIS

The latest research findings from a team of modellers and epidemiologists at Oxford University's Nuffield Department of Medicine and Google Research suggest digital contact tracing, such as that based on Google and Apple's Exposure Notification System (ENS), can help to control the epidemic at low levels of app uptake.

https://www.ox.ac.uk/news/2020-09-03-new-research-shows-tracing-apps-can-save-lives-all-levels-uptake#

Tableau 1: Fraction de transmission évitée selon le pourcentage d'adoption de l'application StopCovid pour un ratio de reproduction=1.35 et un taux d'infection des contacts notifiés de 12.2%.

ADOPTION (a)	**REDUCTION DE TRANSMISSION** $F(a, R_t = 1.35, i = 12.2\%)$
4%	**5%**
5%	6%
10%	12%
15%	18%
20%	25%
25%	31%
30%	37%

https://www.epicx-lab.com/covid-19.html

- **Proximity discovery**: users exchange ephemeral ID over Bluetooth
- **Infected User Declaration**: when a user is tested positive
- **Exposure Status Notification**: exposed users are notified

The 2 architectures!

Why a centralized Architecture?

Reason1: *Health Authority should control the Score computation and Notifications!!*

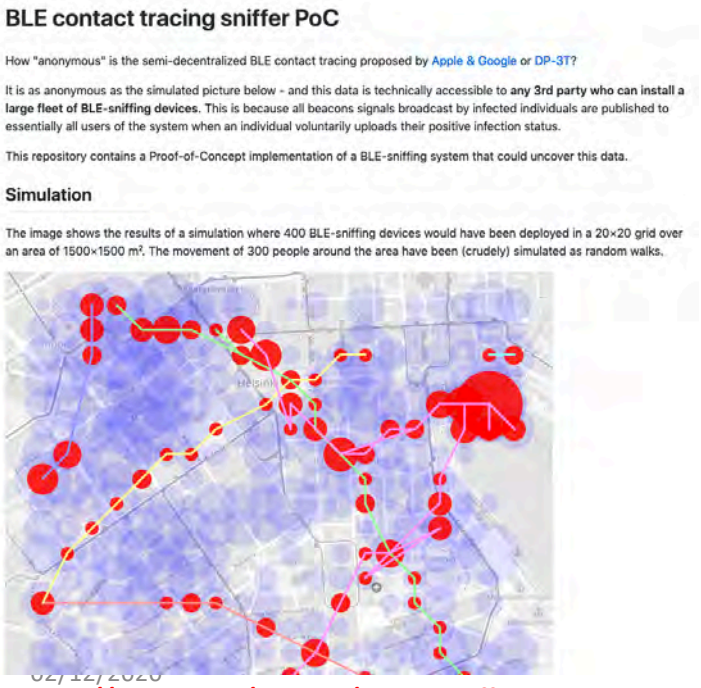
- Several studies by epidemiologists have shown, the health authority should [1]:
  - control when and how the notifications are sent to people
  - should be able to adapt quickly and constantly how the risk scores are computed based on the feedback results and the pandemics evolution

  => this can *only be performed centrally*!

[1] Fraser and all, "Digital contact tracing: comparing the capabilities of centralised and decentralised data architectures to effectively suppress the COVID-19 epidemic whilst maximising freedom of movement and maintaining privacy."

Why a centralized Architecture?
Reason2: *Decentralizing Notification (and PII in general) is too dangerous!*

- Anyone can re-identify and trace all infected nodes!
- You basically have **to trust everybody (including authorities)**

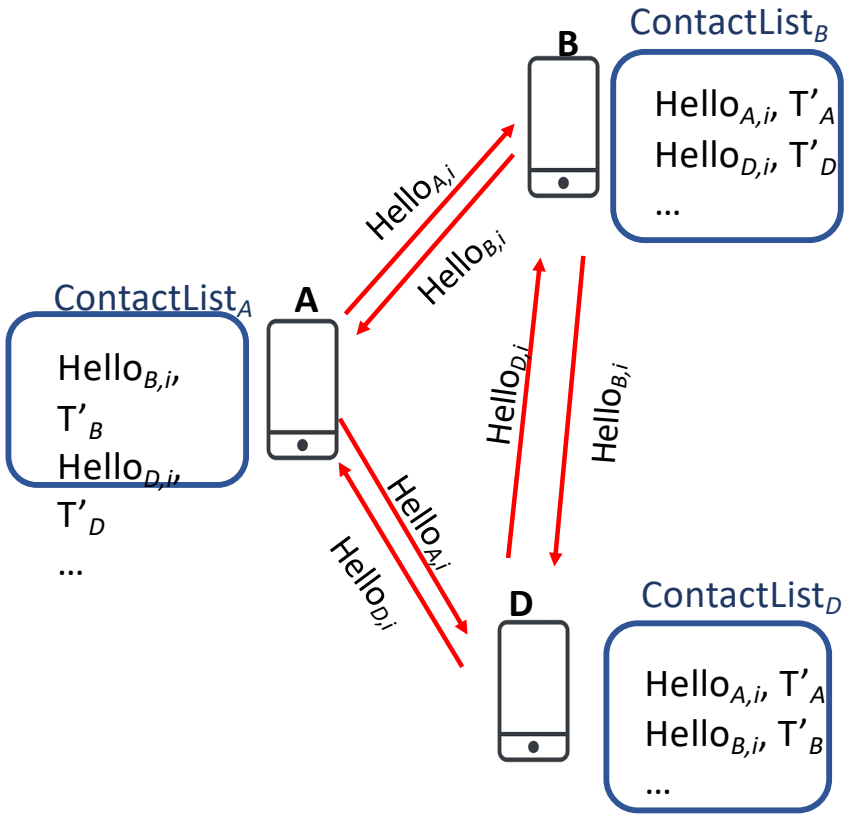


https://github.com/oseiskar/corona-sniffer

https://www.coronadetective.eu

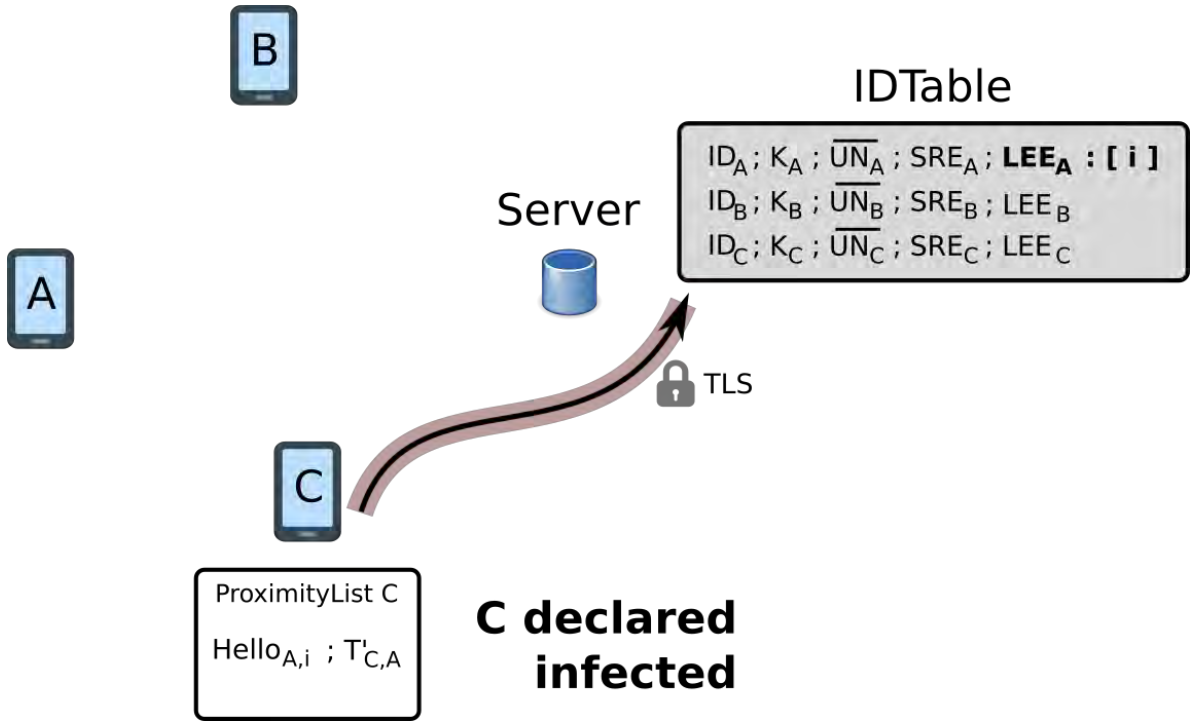
ROBERT

1. **Node configuration:** Nodes get configured with pseudo-identifiers, EphIDs
2. **Proximity discovery**: Users broadcast their Ephemeral IDs and collects the EphIDs of encounters
   - Ephemeral IDs are generated by a server
   - App stores Hello messages it encounters in a list.



ROBERT(2)

3. **Infected User Declaration**: When a user is tested positive, he uploads his lists of collected HELLOs msgs (ephID of his contacts)
   - the server keeps a list of exposed IDs (and break the social graph)

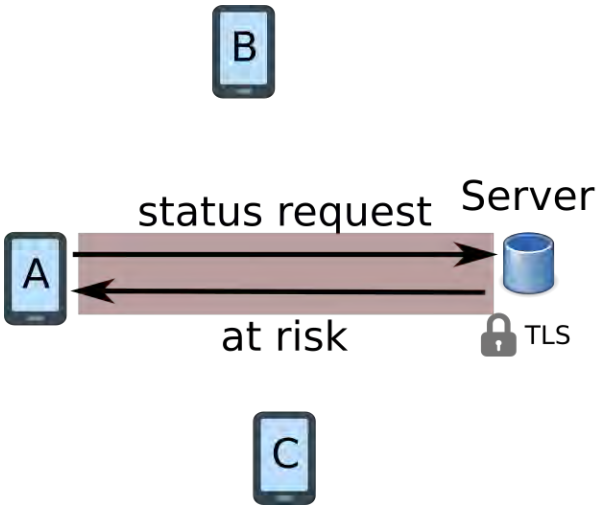


ROBERT(3)

4. Exposure Status Notification:

Each user (app) queries the server regularly to check whether any of his ephIDs are in the list of exposed IDs

- Server **computes** an exposure risk score based on contacts (RSSI, time of exposure, etc)
- **Reply** to client with 1 or 0



IDTable

ID_A ; K_A ; **UN_A** ; **$SRE_A = i$** ; LEE_A: [i]
$\overline{ID_B}$; K_B ; UN_B ; SRE_B ; LEE_B
ID_C ; K_C ; $\overline{UN_C}$; SRE_C ; LEE_C

What about the Big Brother Risk?

What about the Big Brother Risk?

1. We are not Facebook!
   - We are not collecting location, health/sensitive, behavioral data…
   - We don’t target, profile users
   - We don’t manipulate users/ elections/ democracy!
   - We don’t distribute nor monetize data!

What about the Big Brother Risk?

1. We are not Facebook!
   - We are not collecting location, health/sensitive, behavioral data…
   - We don't target, profile user
   - We don't manipulate users/ elections/ democracy!
   - We don't distribute or monetize data!
2. We **only** collect Pseudo-Identifiers
   - We remove all social graph information
   - We apply data minimization
   - Everything is transparent and audited
     - We are regularly audited by DPA (CNIL) and ANSSI (security agency)
   - We aim at **helping people**, fight against the virus… not exploit them!

What about the Big Brother Risk? (2)

CAPITALISM SURVEILLANCE by private companies

!=

Health monitoring by state health autorities!

What about the Big Brother Risk? (2)

CAPITALISM SURVEILLANCE by private companies

!=

Health monitoring by state health autorities!

Privacy does not mean "taking data away from health authorities" but to build a trust relationship with them!!

MIT Review Rating (Nov. 2020)

MIT Technology Review Covid Tracing Tracker

Search...

ɔcation	Name	Notes	Voluntary	Limited	Data destruction	Minimized	Transparent	Tech
France	TousAntiCovid	Like the UK and Norway, France negotiated with Apple and Google but decided against using their standards	★	★	★	★	★	Bluetooth

https://www.technologyreview.com/2020/11/23/1012491/contact-tracing-mandatory-singapore-covid-pandemic

Current Work

- Develop a **hybrid** architecture (DESIRE):
  1. Centralized risk score and notification
  2. Decentralized temporary ID generation and management…
- Add **Backward** Contact Tracing into TousAntiCovid
  - Extend ROBERT
  - Develop next schemes based on QR codes for events.

5 lessons learned…

Lesson5:

Huge gap between Privacy research/theory and Privacy engineering

Decentralization and Personal Data Processing should be avoided!

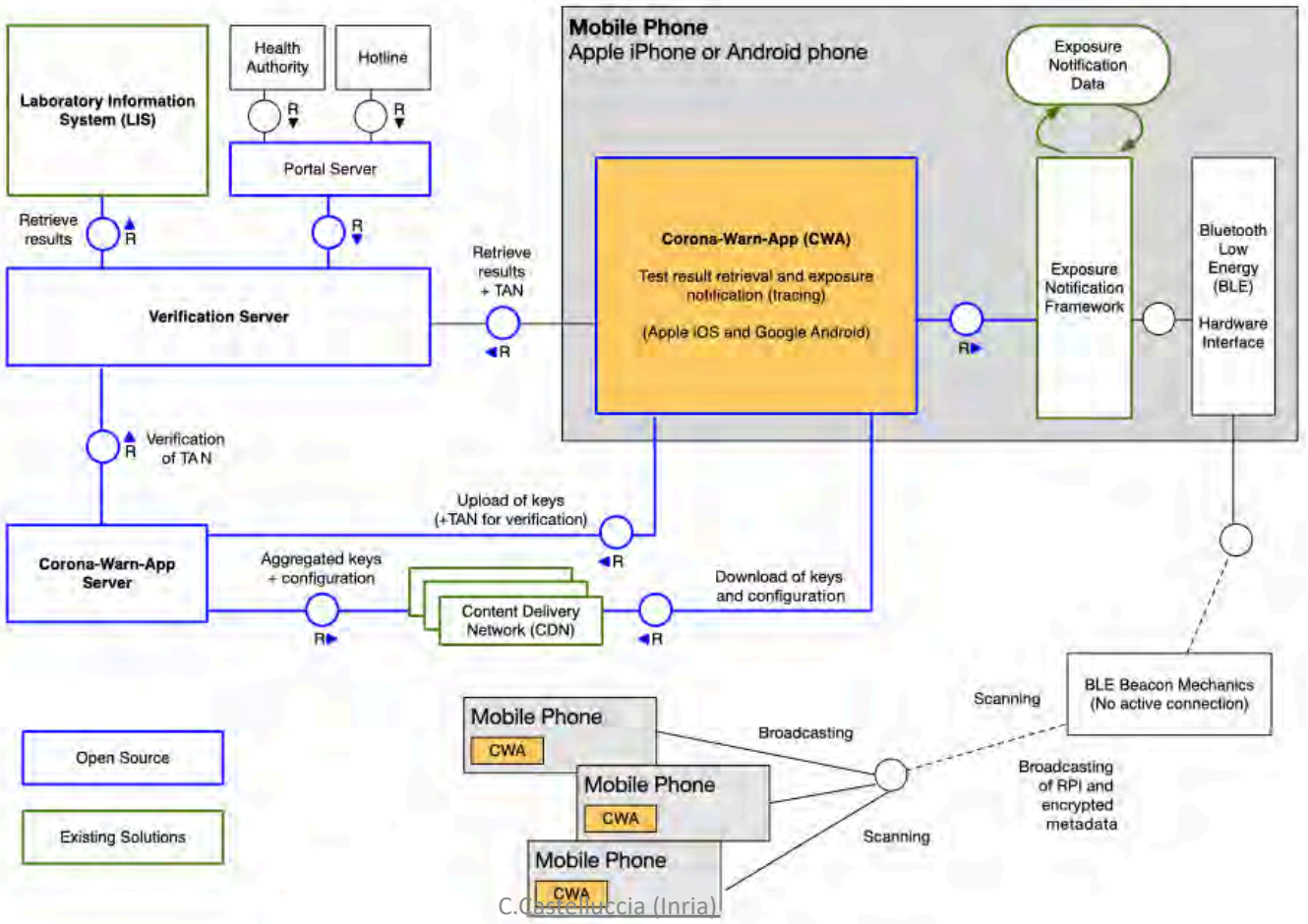
- **According to Privacy Community, decentralization has several limitations [2]:**
  1. *"Fundamental **Tradeoff** between availability, security, privacy*
  2. *"Most decentralized systems end up using **servers** for scalability and abuse control"*
  3. *"They make **unrealistic assumptions about** device security"*

*[2] **Troncoso** and al., "Systematizing Decentralization and Privacy: Lessons from 15 Years of Research and Deployments", PETS 2017*

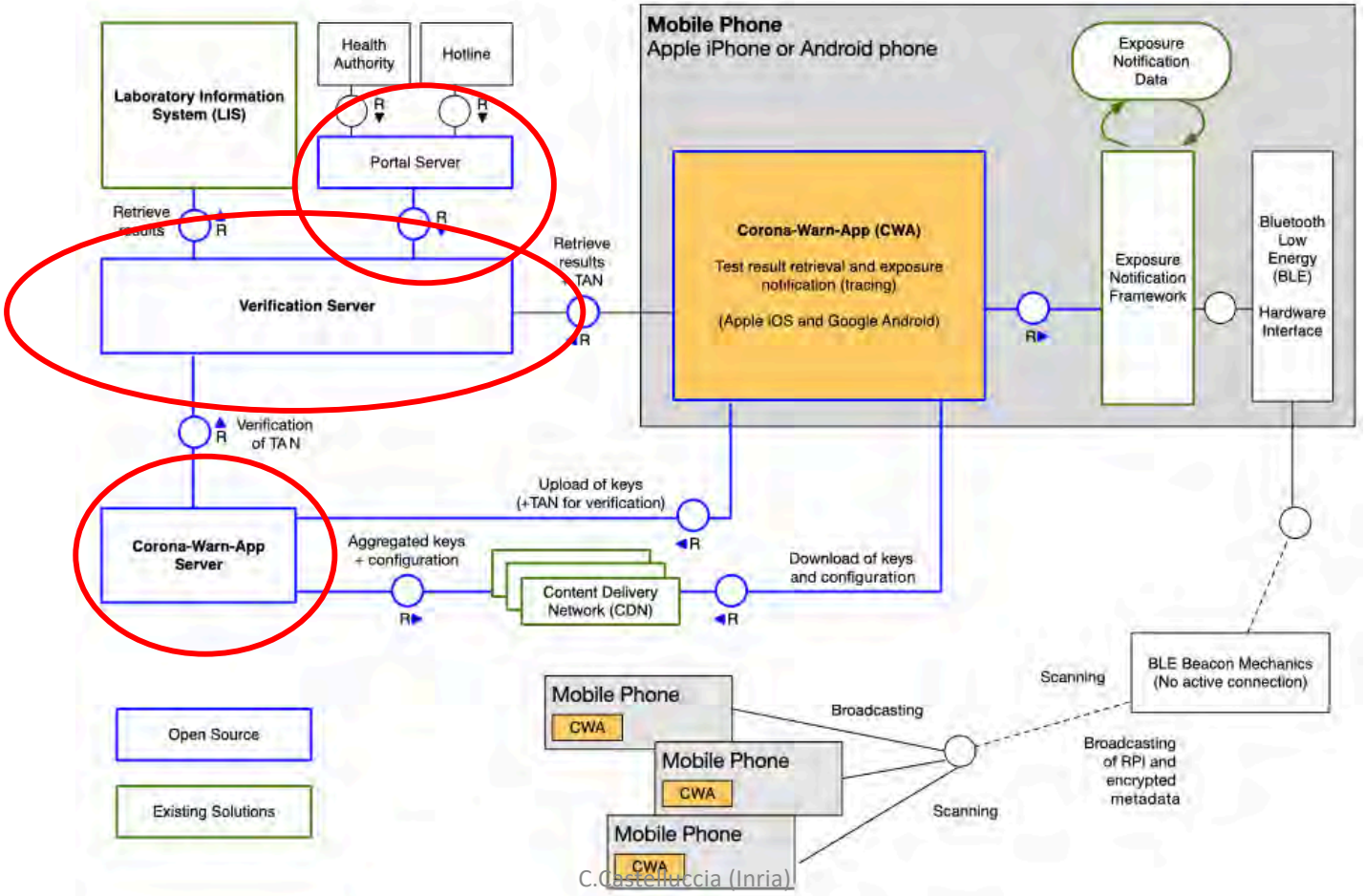
Lesson4:

Decentralized + Centralized = Centralized !

The German so called “decentralized system”



The German so called “decentralized system”



Lesson3:

We need to promote (Privacy-Preserving) Evaluation-by-design

Lesson2:

Users participation/engagement is essential!

- "chicken-and-egg" problem: The system works only if a lot of people buy into it, but people will buy into it only if they know it works.
- "There's a general belief that some people want to load the app so that they can be notified if someone else was positive, in a self-serving way," he said. "But if they're positive, they don't want to take the time."
- For example, "only 13 percent of people with confirmed cases in Switzerland used the app to alert their contacts from July to September"

https://www.cpr.org/2020/11/19/the-biggest-bug-for-coronavirus-exposure-apps-the-people-using-them/

Lesson1:

CODE is Law (Lessig)!

CODE is Law (Lessig)!

- Google-Apple decided for Europe (and others) what was possible or not in order to fight the Virus!
- They made some security assumptions:
  - Protecting social graph is more important than protecting infected users!
  - Without discussing/negotiation with governments…
  - It was a “take it or leave it” approach!
- This was possible because they own the CODE!
- Is it acceptable that private companies decide unilaterally about health policies?

CODE is Law (Lessig)!

- Google-Apple decided for Europe (and others) what was possible or not to fight the Virus!
- They made some security assumptions:
  - Protection social graph is more important than protecting infected users!
  - Without discussing with government…
  - It was a “take it or leave it” approach!
- This was possible because they own the CODE!

- Where is EU sovereignty?

THANKS FOR YOUR ATTENTION!

Claude.Castelluccia@inria.fr

"talking is easy, doing difficult"

My Message to EU Institutions

Shusha Zuboff (author of “Surveillance Capitalism”):

*“The information empire led by Google and Apple took their **unaccountable power** without collaboration with governments, developed their own approach and they gazlighted this approach…**they create a polemic that says that our app is the privacy app and what the state is trying to do is to spy on you**…and undercut the legitimate need of public health authorities that operate under democracy, leaving countries like Germany, France, UK just in a set of intolerable constraints! **This is intolerable and incompatible with democracy!**”*

https://www.youtube.com/watch?v=NOKxAIyPLpo
https://www.brookings.edu/techstream/the-dangers-of-tech-driven-solutions-to-covid-19/