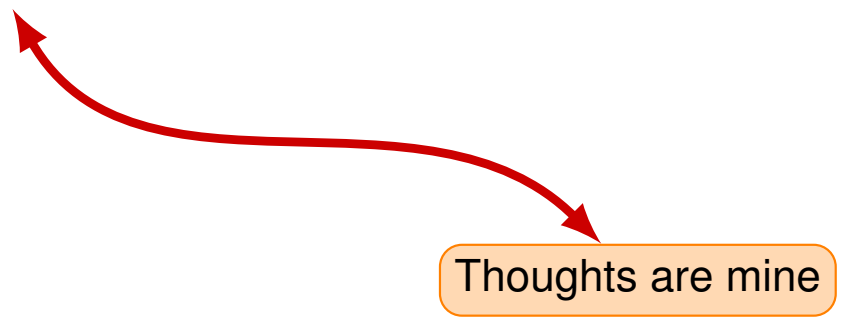
Lessons from SwissCovid

The Dark Side of SwissCovid

Serge Vaudenay, EPFL, Switzerland
Martin Vuagnoux, base23, Switzerland



Law on Epidemics

(The Pandora Box)

After a positive diagnosis, obligation to report the identity of diagnosed people and the people they may have contaminated.

> ***Loi sur les épidémies, LEp***
> ***Art. 33 Identification et information***
> *Les personnes malades, présumées malades, infectées, présumées infectées ou qui excrètent des agents pathogènes peuvent être identifiées et des informations leur être communiquées.*

Limitation: this measure must be "necessary and reasonable"

→ **we are talking about reducing privacy (and other human rights)**

(Human) Contact Tracing

- get test results from health department
- contact people
- must establish trust relationship
- explain confidentiality, how data is used and shared
- ask them to recall the names of every recent encounters
- advise to self-quarantine and explain protocols
- need empathy

$\rightarrow$ tedious

$\rightarrow$ contacts in public transport are hard to identify

$\rightarrow$ need for automated contact tracing

DP-3T (non-)Goals

Purpose:

- “alert users who have been in close proximity to a confirmed COVID-19 positive case for a prolonged duration”

Non-goals:

- track positive cases
- locate clusters
- share data with epidemiologists (used to be)

`https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf`

Technological Design Choices

- on smartphones
- detect proximity using Bluetooth only
- “decentralized”

From DP-3T to SwissCovid

- early April: within PEPP-PT
- split from PEPP-PT to promote decentralized systems
- Bluetooth access constraints on smartphones
- Apple-Google say they will support decentralized systems
- surprise: they implement it
  $\rightarrow$ what is left to the app:
  - communicate to servers (obfuscation)
  - interact with user (graphic interface)
  - choose parameters for risk evaluation

Political Basis

LEp Art.60a (parliament vs gov)

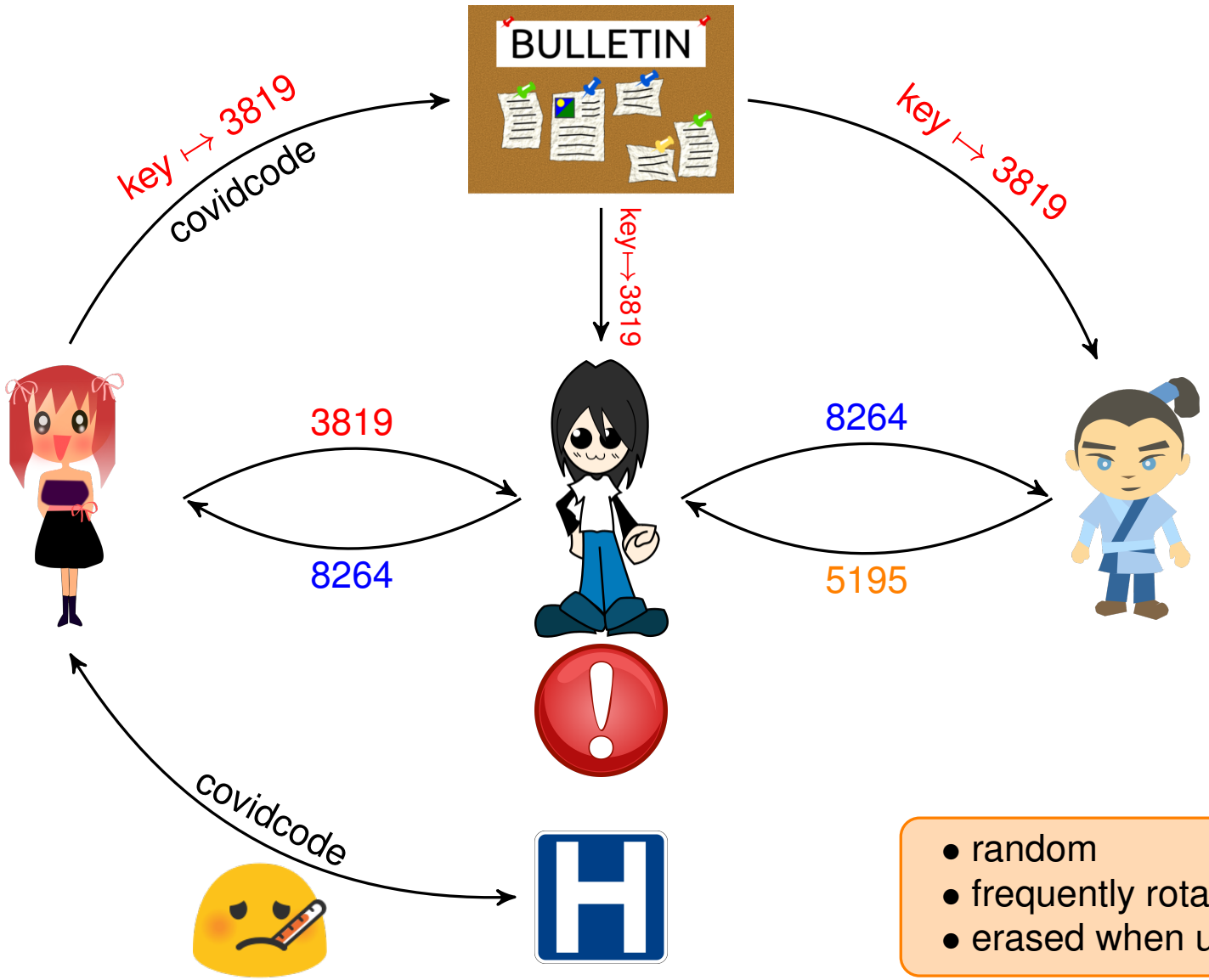
- other use forbidden
- voluntary - discrimination based on usage is forbidden
  exception: free COVID test if notified
- users should never be identified
- decentralized
- no geolocalisation
- data are erased when no longer necessary
- source code public and verifiable for all components
- specs available for all components
- law on data protection applies
- government in charge of details
- sunset when no longer useful or if inefficient

`https://www.admin.ch/opc/fr/classified-compilation/20071012/index.html#a60a`

Which Choice?

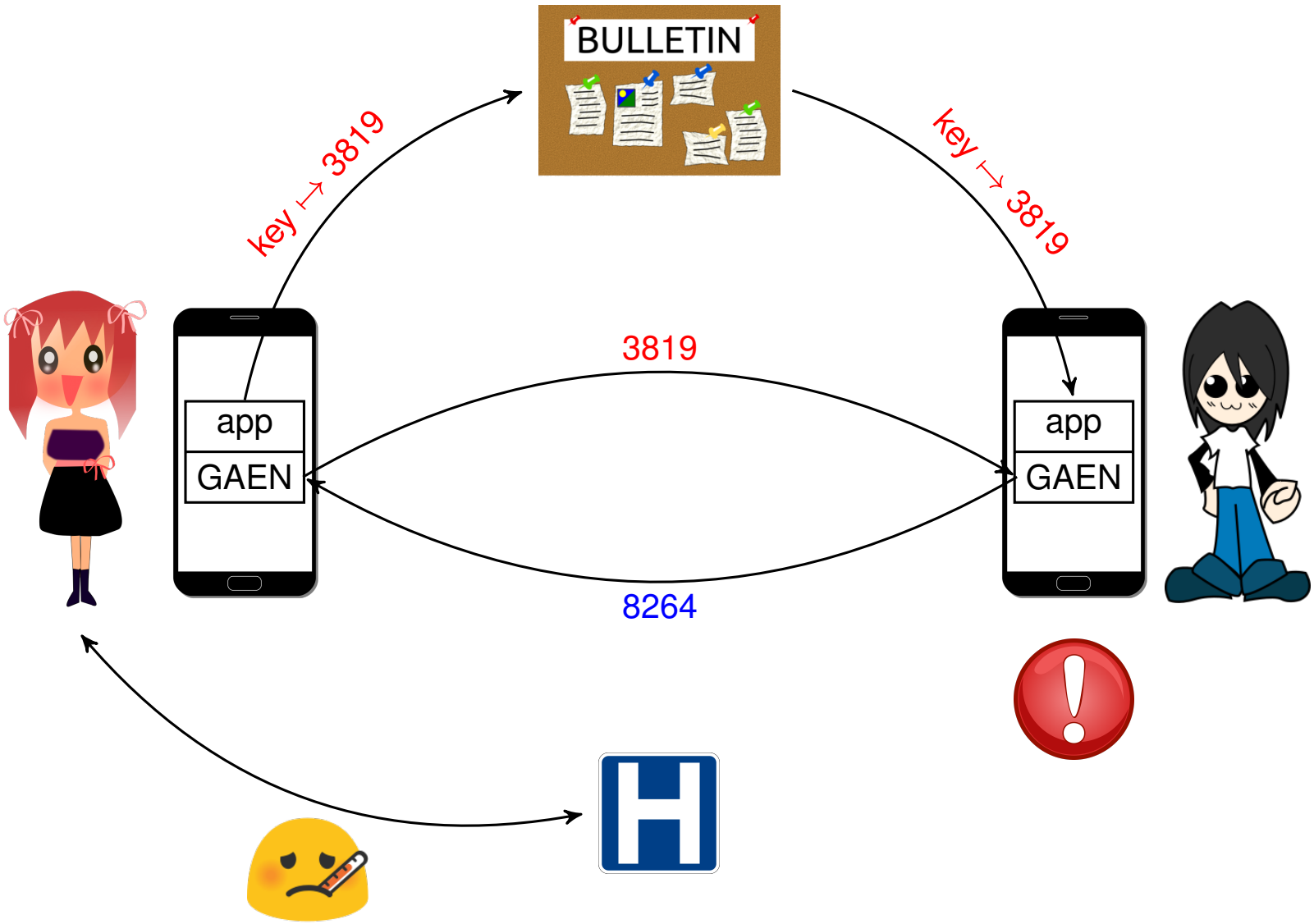
- install / not install
- activate / not activate
- if notified: react / not react
- if diagnosed: report / not report
  (+ select which days to report)
- no choice for quarantine/isolation if ordered by authority

Decentralized Contact Tracing



- random
- frequently rotated
- erased when useless

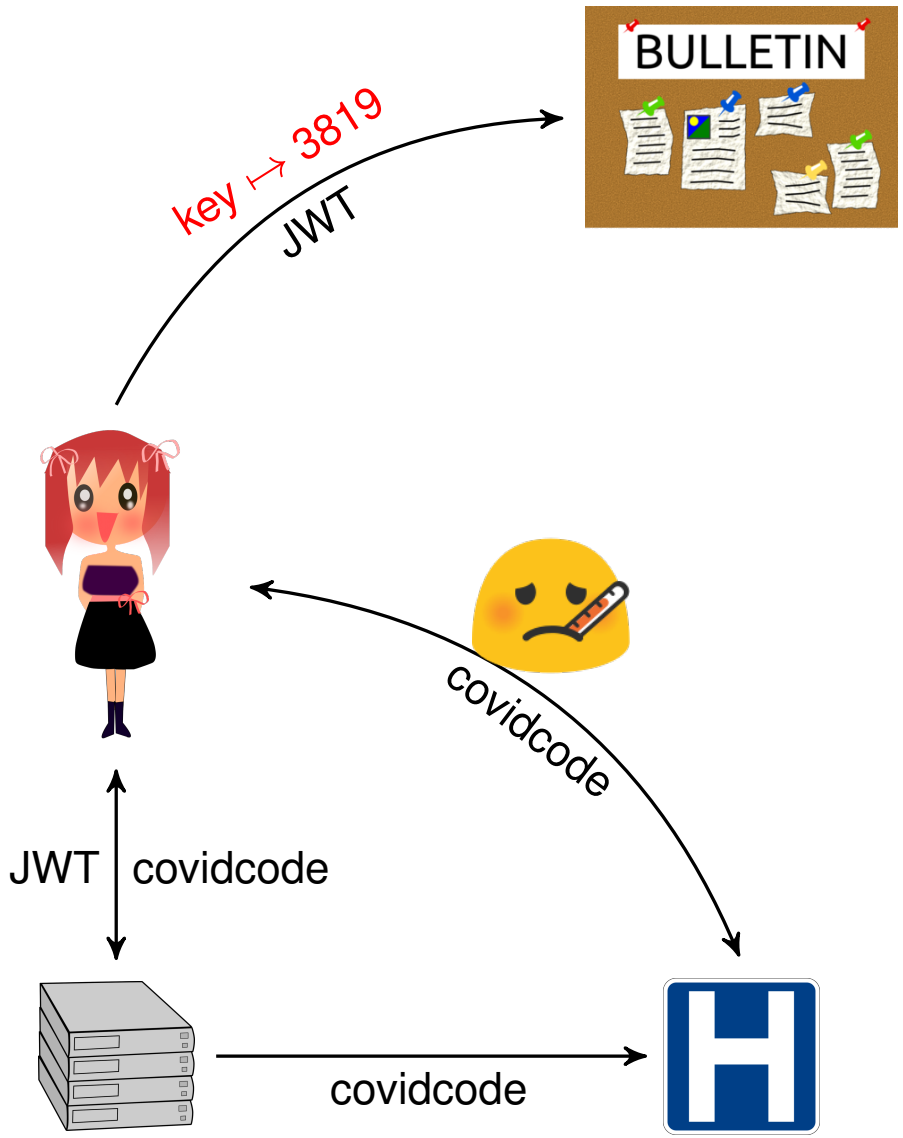
App vs GAEN/ENS



Done by GAEN/ENS

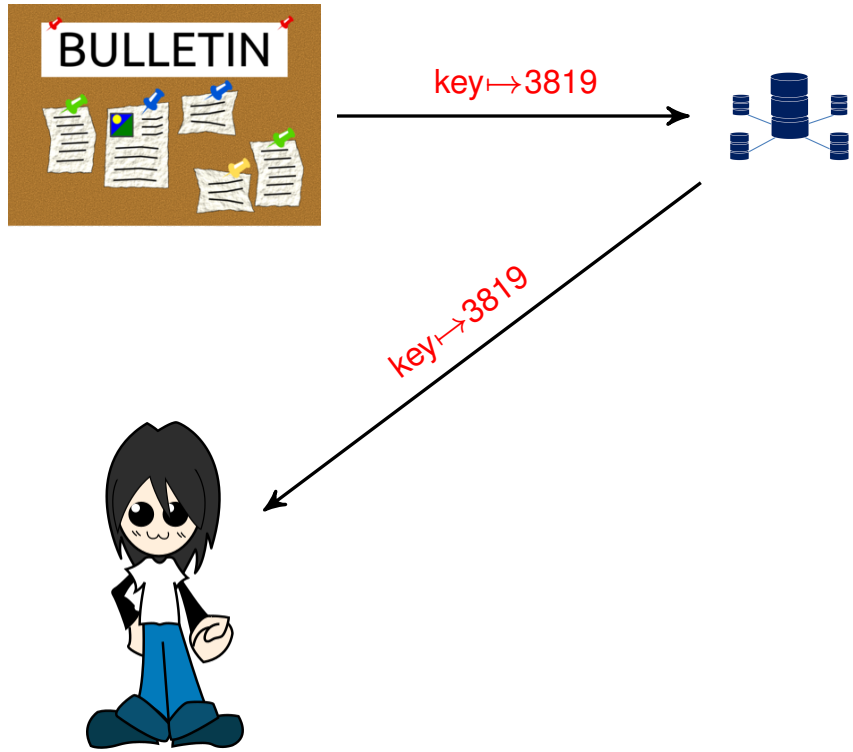
- generation of a new key of the day
- exchange of ephemeral identifiers via Bluetooth
- storage of received ephemeral identifiers
- matching of downloaded diagnosed keys with storage

Upload to Server



- 12-digit covidcode
- valid one time for 24h
- random fake uploads

Download from Server



- CDN (Amazon)
- content signed

False Exposure Notification

“Lazy Student Attack”

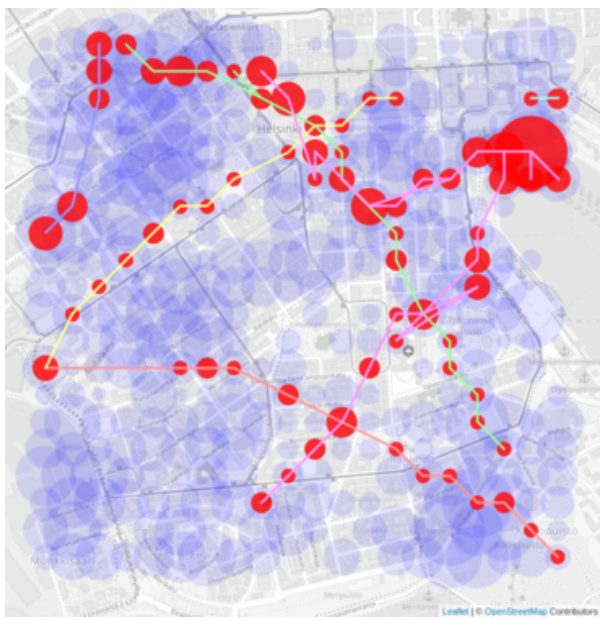
Goal: make people receive an exposure alert

- **Terrorism/activism**: a group of people sync on beacons to massively broadcast and one sacrifices to get sick
- **False report submission**:
  - get a positive test
  - buy a covidcode to a diagnosed person
  - corrupt the medical infrastructure
  - set JWT verification algorithm to null...
- **Replay/relay** broadcast from a person going to ER

Privacy of Reporting People

“Paparazzi Attack”

- **Paparazzi attack:** spot celebrities who get infected
- **Nerd attack:** enrich app storage to read more data
- **Militia attack:** share enriched app storage
- **Hotel/Company/Shop:** identify sick visitors/employee
- **+ video-surveillance:** see past movements of sicks
- **Bluetooth sniffer:**



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

Privacy of SwissCovid Users

Mass Surveillance

- **Chase** users (like Pokemons)

  [Bénédicte@Vigousse]
- **Sniffer**
- **Collect** beacon+location+time+extra and sell them

Does SwissCovid Work?

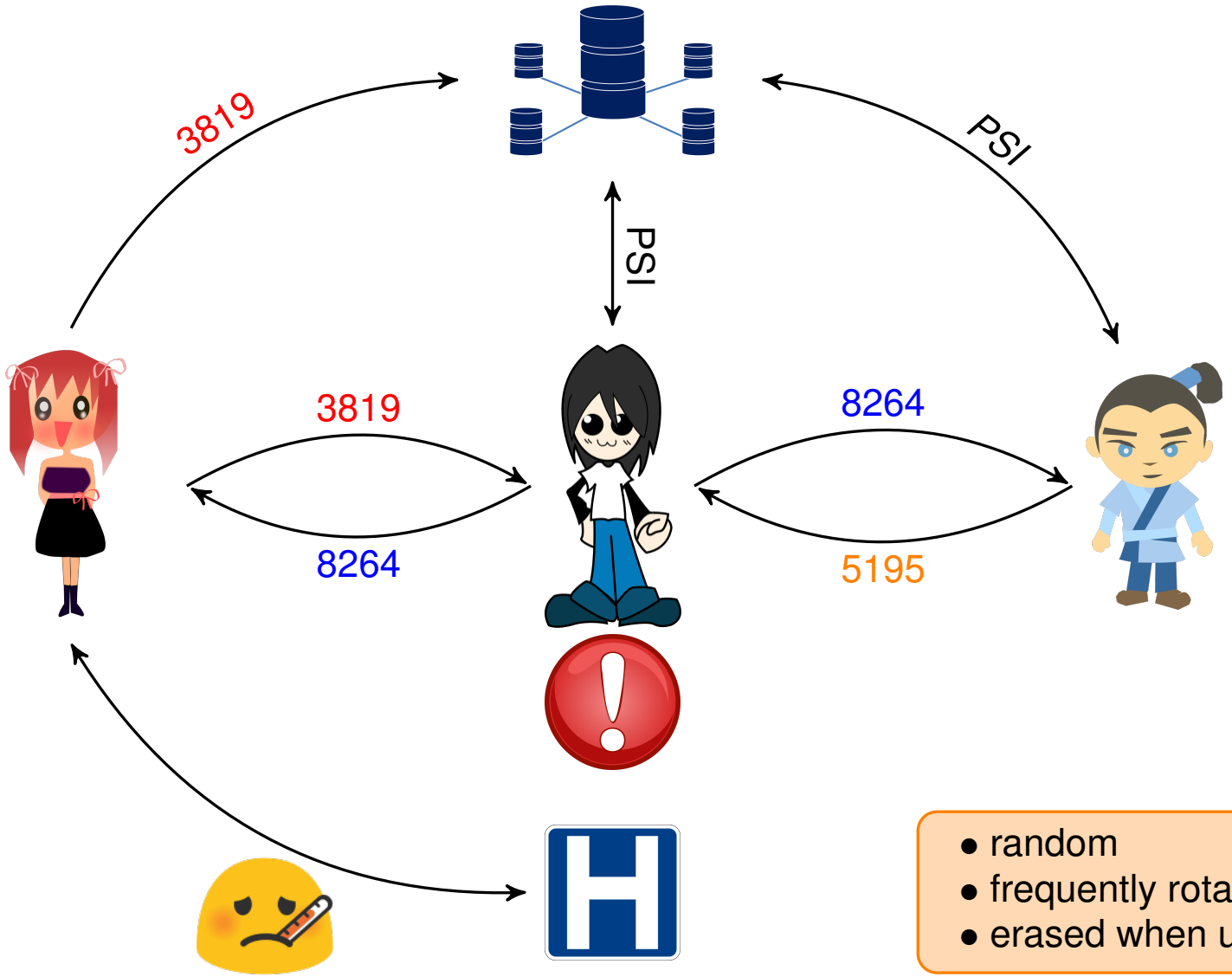
False Positives/Negatives

- **Goal**: notify if the total of proximity (up to 1.5m) to a reported user exceeds 15 minutes during the same day
- Distance is guessed based on signal attenuation
  $\rightarrow$ It is highly imprecise
- Reported cases of no proximity discovery (false negative)
- Leith-Farrell 26.6.2020:
  Measurement-Based Evaluation Of Google/Apple Exposure Notification API For Proximity Detection In A Light-Rail Tram
- Parameters have been increased to more sensitivity

Alternative 1

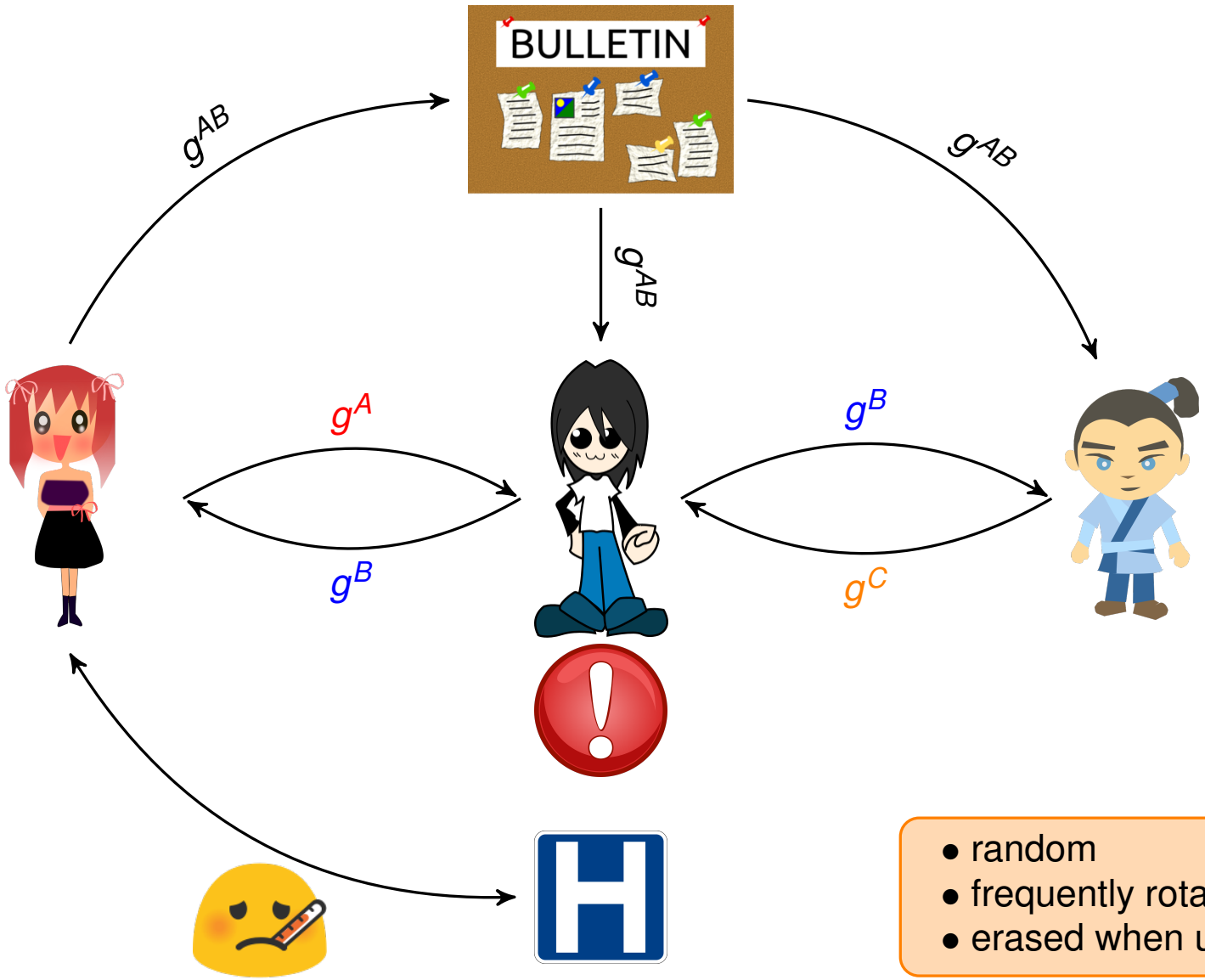
Alternative 2

Epione: Decentralized + PSI



- random
- frequently rotated
- erased when useless

Pronto-C2: DH + Blockchain



- random
- frequently rotated
- erased when useless

A Pact with Apple/Google

[Faust]

On Apple/Google Overtaking

- Gov made an ordinance to except GAEN from public src
- some sample/partial code was (lately) released
- can be updated without notification
- Android: part of Google Play Services which send IP address, phone number, email address, IMEI, SIM...
- now Apple is giving a weekly notification to users (conflict with the app's notification)
- soon: app to be fully integrated in GAEN (EN Express) (easier for everyone - not for citizens)

Legality

- **LEp**:

the law	**real world**
voluntary	app or mask mandatory
no discrimination	social pressure
public verifiable src	opaque GAEN
public specs	no specs

- **Medical device**
- **Data protection**

A Few Bugs

- weird errors
- Bluetooth receives nothing on some phones
- fake keys with postdated validity by authority
- bypassing JWT verification

...but also

- covidcode delivered 2 days later
- relevant period is more than 2 days
- Swiss law on privacy insufficient for interoperability

Oops

Adoption

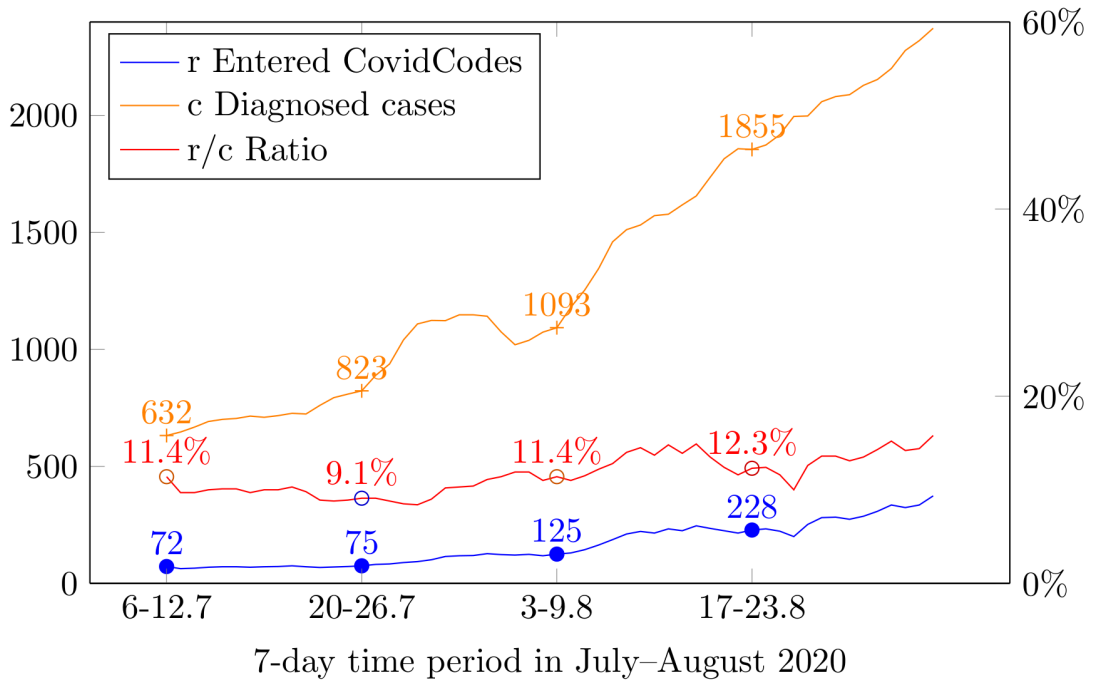
- about 18% of population
- 10–15% of diagnosed people are SwissCovid reporters
- $\rightarrow$ 2% of contaminating proximities to be noticed??

current strategy to solicit adoption

- weird SMS sent by mobile operators
- weird TikTok campaign
- proposal by economists: opt-out

Usefulness

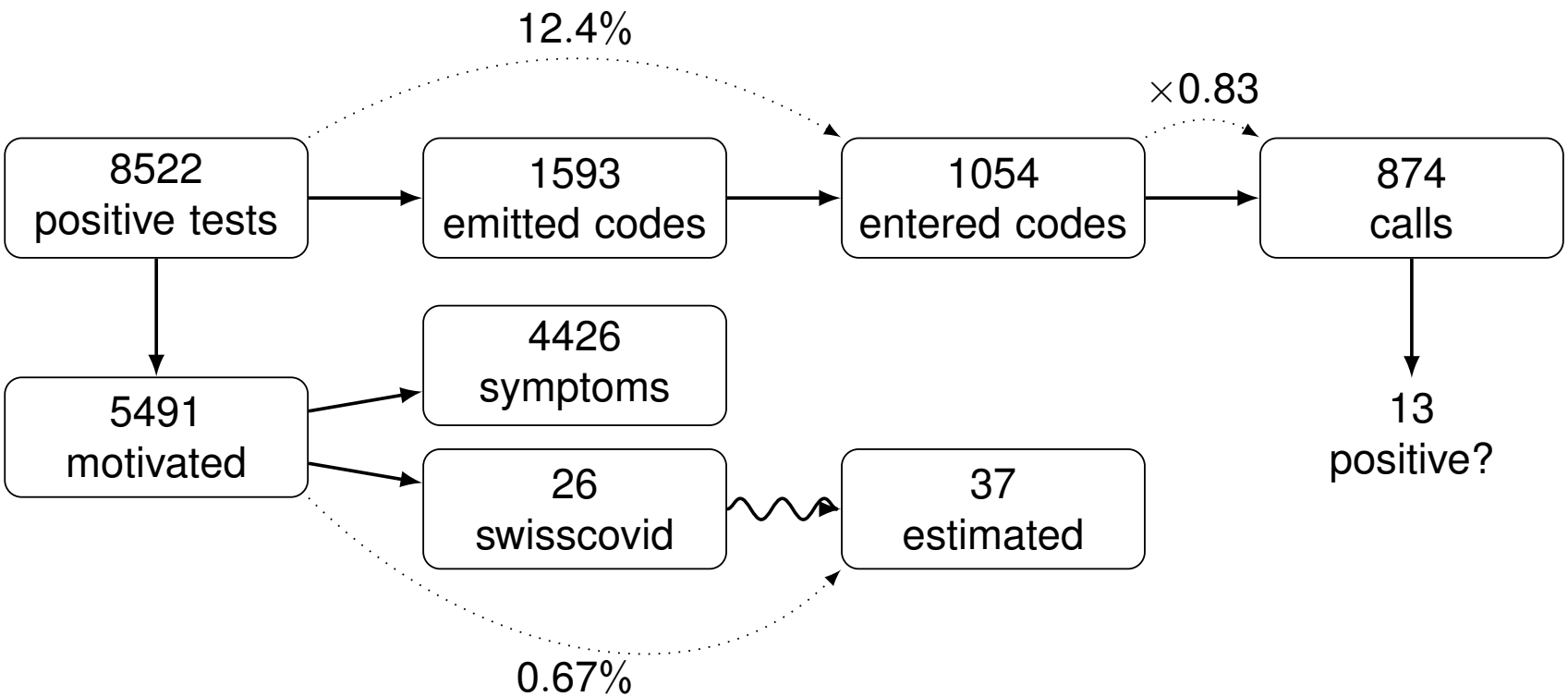
- app gives little data
- trick to count “activations”
- counting submitted reports only



- no way to count notifications
- count calls to infoline
- survey

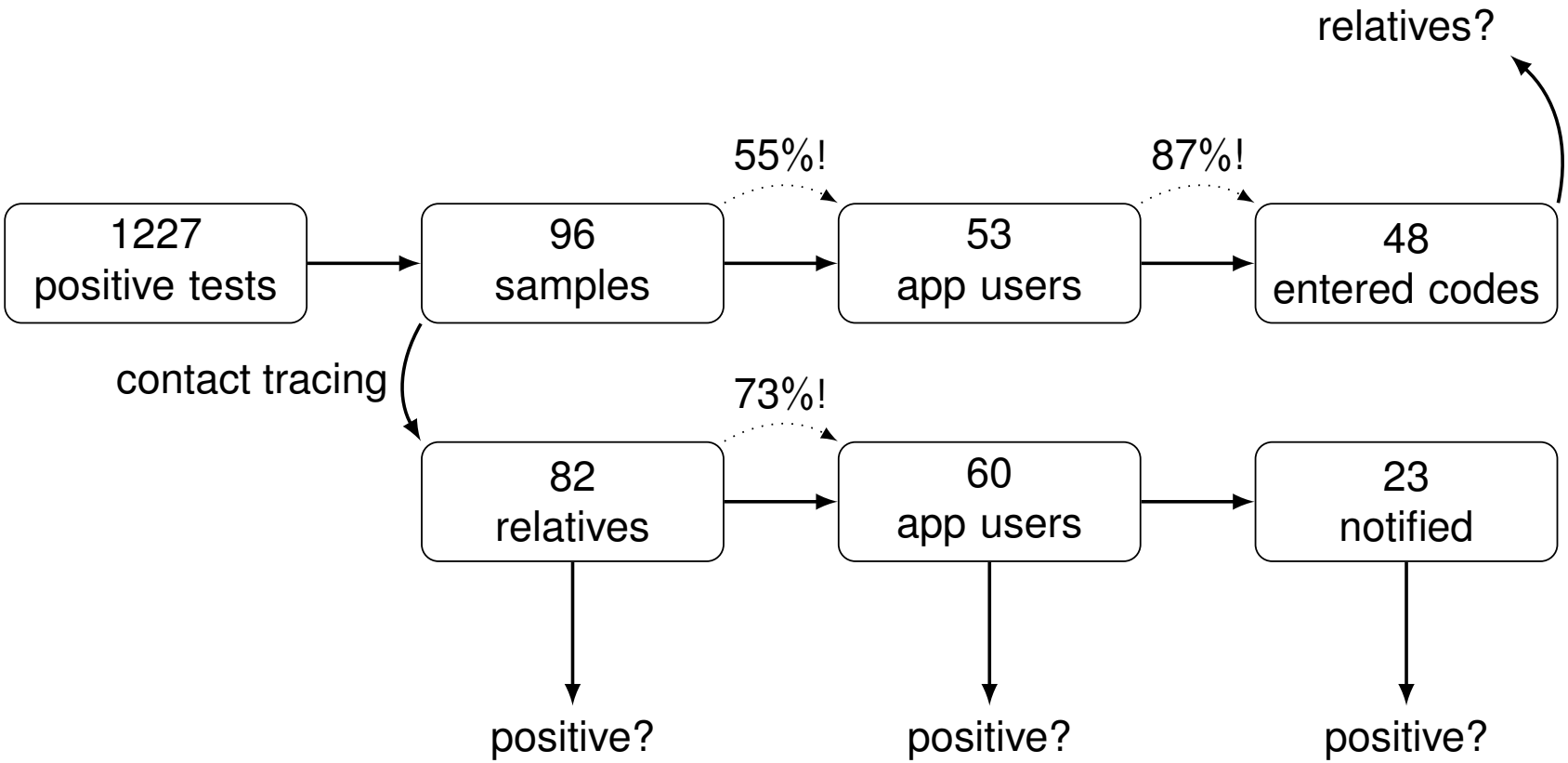
Latest News: Early Evidence of Effectiveness [...]

https://github.com/digitalepidemiologylab/swisscovid_efficacy/blob/master/SwissCovid_efficacy_MS.pdf



The Zurich Cohort

https://github.com/digitalepidemiologylab/swisscovid_efficacy/blob/master/SwissCovid_efficacy_MS.pdf



Why no More Users?

- privacy?
- not all people have a smartphone
- not all smartphones work
  - old ones
  - Chinese new ones
  - open Android or deGoogled
- people have overloaded smartphones or poor battery
- people don't want to turn Bluetooth on
- it is a boring app
- the app can only give bad news or put people in troubles
- quarantine means income loss
  - for free lance people
  - for "faulty" quarantines

  others: $\min(\text{income} \times 80\%, \text{bound})$ for 10 days out of 14

From DP-3T to SwissCovid: Missed Goals

original DP-3T		current SwissCovid
(data to epidemiologists)	$\rightarrow$	no way
open-source	$\rightarrow$	GAEN-based
decentralized	$\rightarrow$	GAEN-controlled
privacy-preserving	$\rightarrow$	well...
completeness	$\rightarrow$	false negatives
precision	$\rightarrow$	false positives
authenticity	$\rightarrow$	relay attacks
interoperability	$\rightarrow$	for next vacations

Does Privacy Matter?

- the law on epidemics allows to take measures against human rights as long as they are

  “necessary and reasonable”

- quote from a Minister from the state of Bern:

  We should definitely know if we want to fight against this pandemic or if we shall be stopped on details about data protection.

  (“Il faudrait quand même savoir si nous voulons combattre cette épidémie ou si nous voulons nous arrêter sur des détails concernant la protection des données.”)

Pierre-Alain Schnegg, 8.8.2020
(About getting the list of passengers flying to Zurich.)

Referendum against the Law on SwissCovid

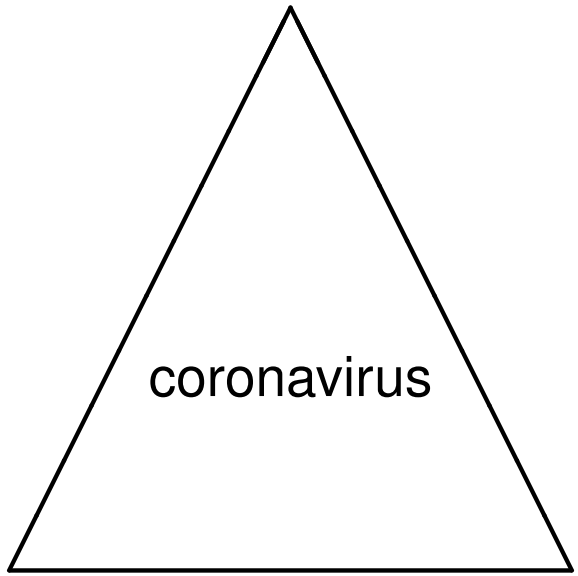
- "**Conspirationists**":
  - there are less deaths than usual – it is just a flu
  - locking down / masks are non-proportional – dangerous
  - Gov is scaring people – media follow
  - too much emphasize on alarming data
  - fake data (death among the youth)
  - next, mandatory vaccine
  - "turn off TV and turn on your brain"

  - nanoparticles in vaccine, interact with 5G
  - WHO is corrupted
  - support to bigPharma
  - working medicine is forbidden
  - Bill Gates is the main sponsor (sometimes Rothschild/Rockefeller)
  - pedophilia, deep state, Q
- **SwissCovid people**:
  -

An Obscene Competition

- fight for toilet paper
- countries fighting to buy masks
- race by research to develop a vaccine
- hacking of research centers
- race by countries to announce a vaccine
- countries pre-empting (non-existing) vaccines

Is There a Pilot on Board?



Science is Failing

- contradicting experts
- conflicts of interest
- bad science
  experts addicted to posting punchlines in social media
  experts taking on-going research as established truth
- fights between experts is now publicly visible
  science now being mocked in media
  starting to sneak on how science works

Ethics in Science

ENRIO: Research integrity even more important for research during a pandemic

- “Researchers should communicate their work on social and other media responsibly, with professionalism and transparency.”
- “Subjective or unfounded interpretations must be avoided and information must not be intentionally omitted.”
- “Eroding the integrity of research undermines the trust of our colleagues, the public and policymakers.”

http://www.enrio.eu/
enrio-statement-research-integrity-even-more-important-for-research-during-a-pandemic/

Conclusion

Much Ado About Nothing

- privacy is the least worry
- usefulness is far from proven
- miscommunication to people
- be careful when playing with the reputation of science

"turn off TV and turn on your brain"
(but use it wisely)

may this nightmare end well!

`https://lasec.epfl.ch/people/vaudenay/swisscovid.html`