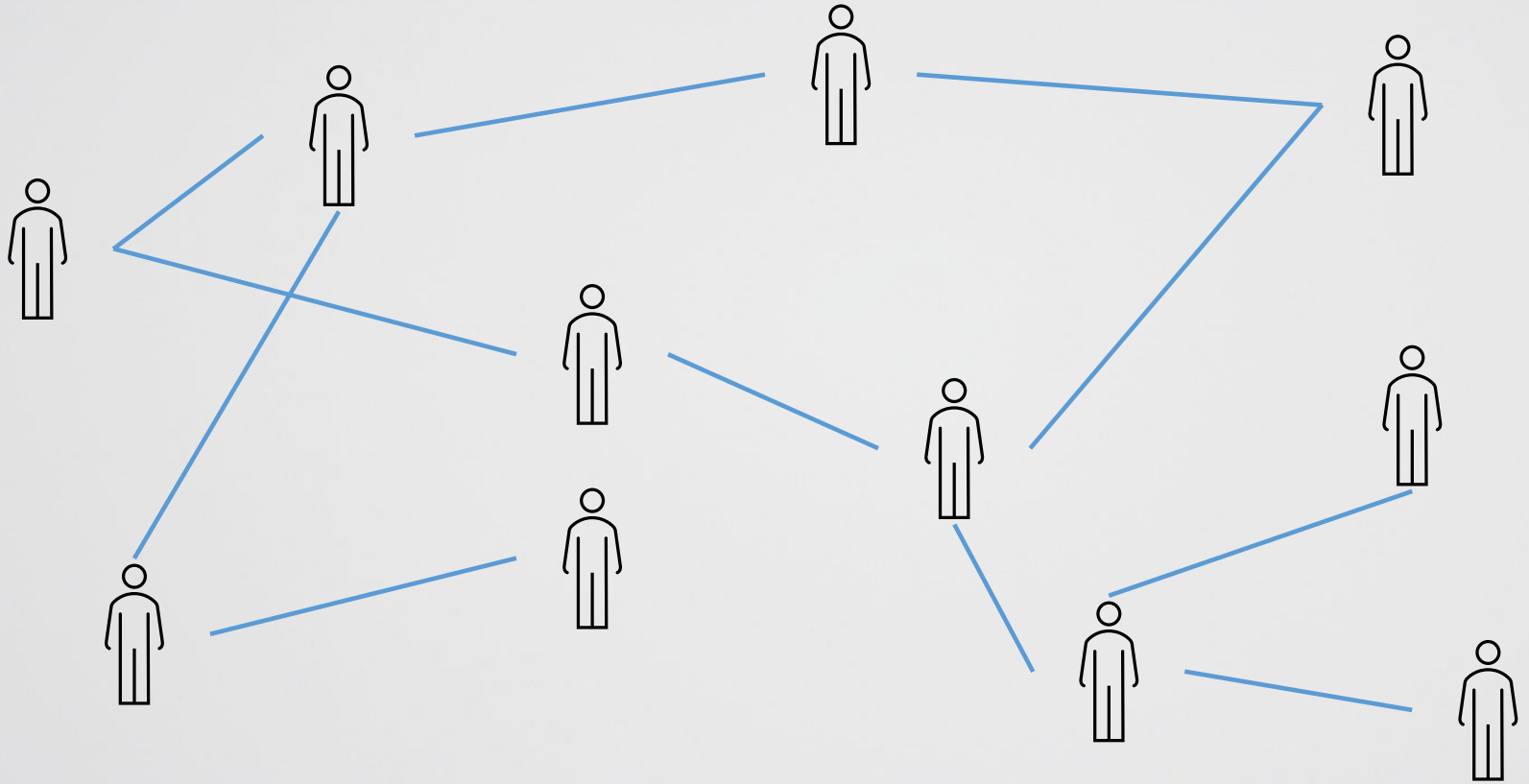
Bluetooth Based Contact Tracing for COVID-19 – The Israeli Perspective

Benny Pinkas Eyal Ronen

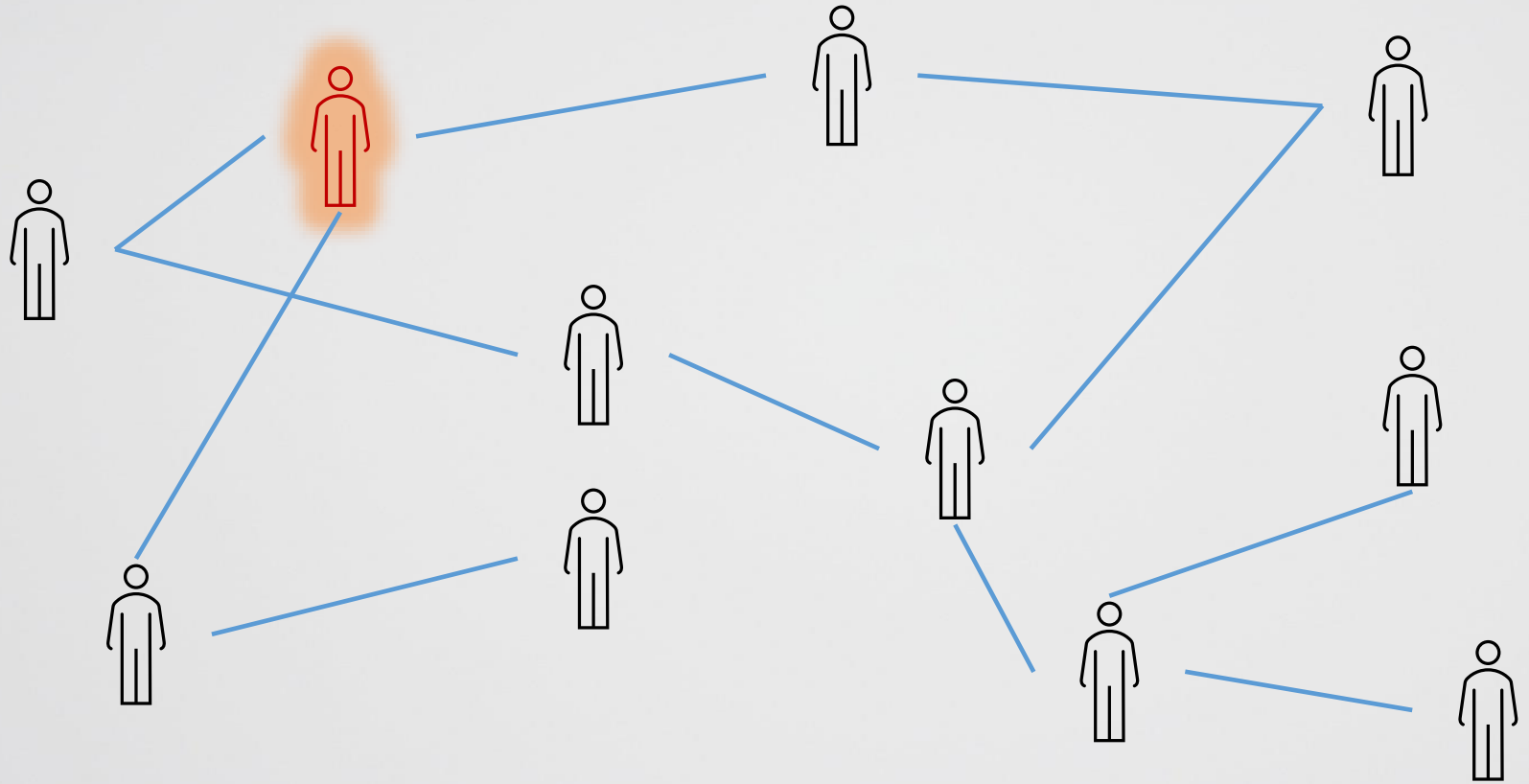
https://github.com/eyalr0/HashomerCryptoRef

BIU Center for Research in Applied Cryptography and Cyber Security

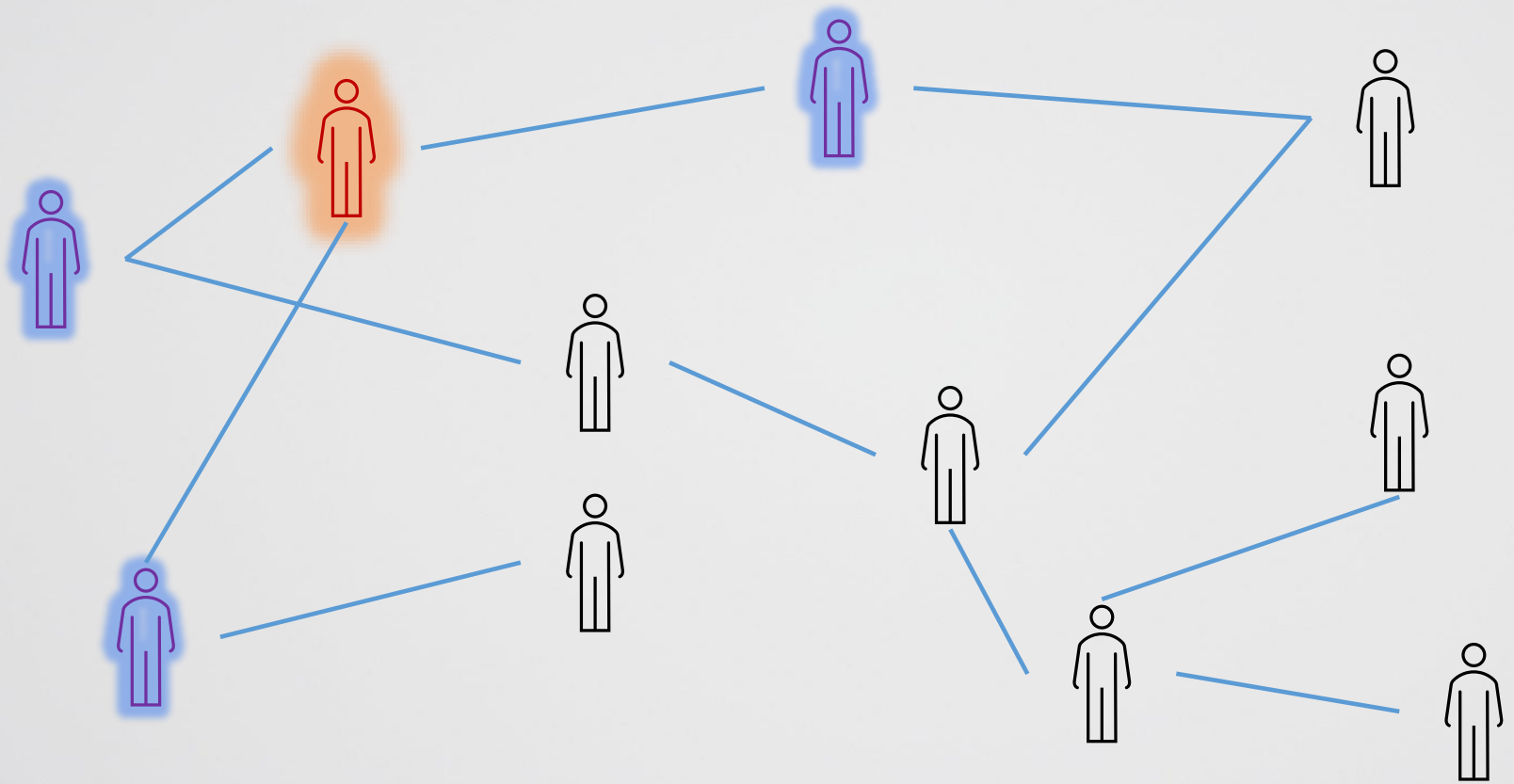
People meet each other



Alice is identified as COVID-19 positive



Need to inform whoever met Alice



Manual Contact Tracing

- Manual epidemiologic interrogation
  - Where have you been?
  - Who you have met?
  - Hard to scale to a large number of new positives

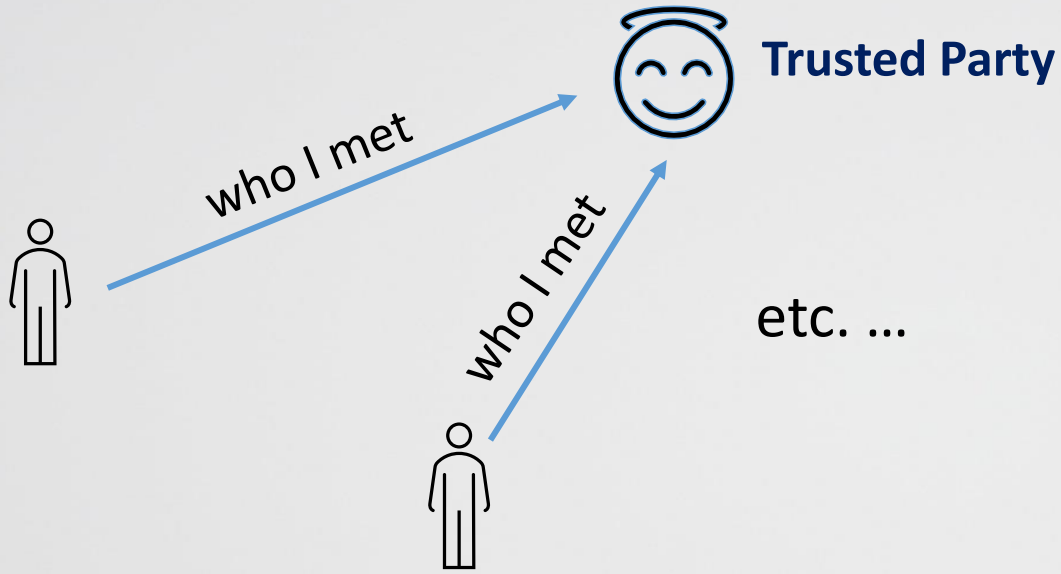
Automated Contact Tracing

- Google, Apple, credit card companies, etc. know where you were, but do not provide governments with information for this specific purpose

- *In Israel, the government asked the security service to perform contact tracing using methods that were developed to track terrorists (cellular data?)*
  - *This is very problematic in terms of civil rights*
  - *And is not sufficiently accurate*

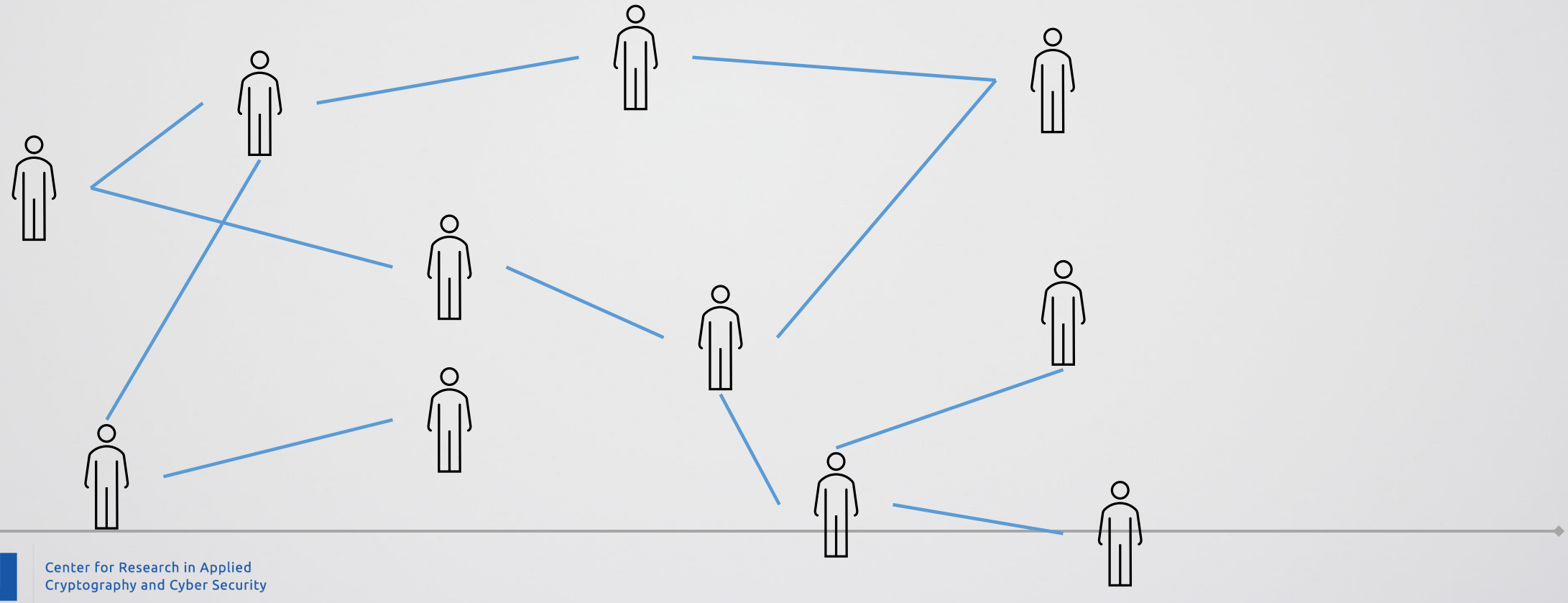
- People do not want the government to track them all the time

In an Ideal World

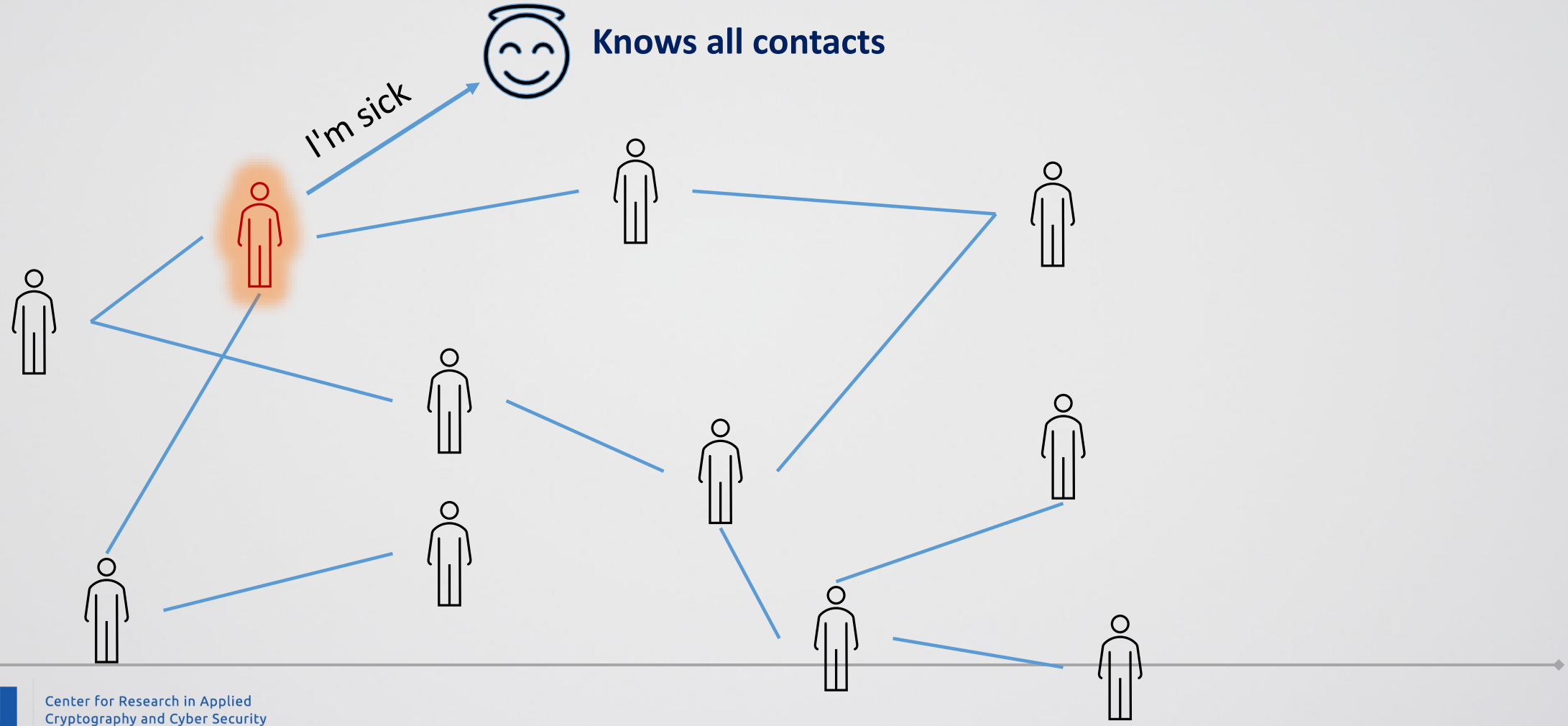


In an Ideal World

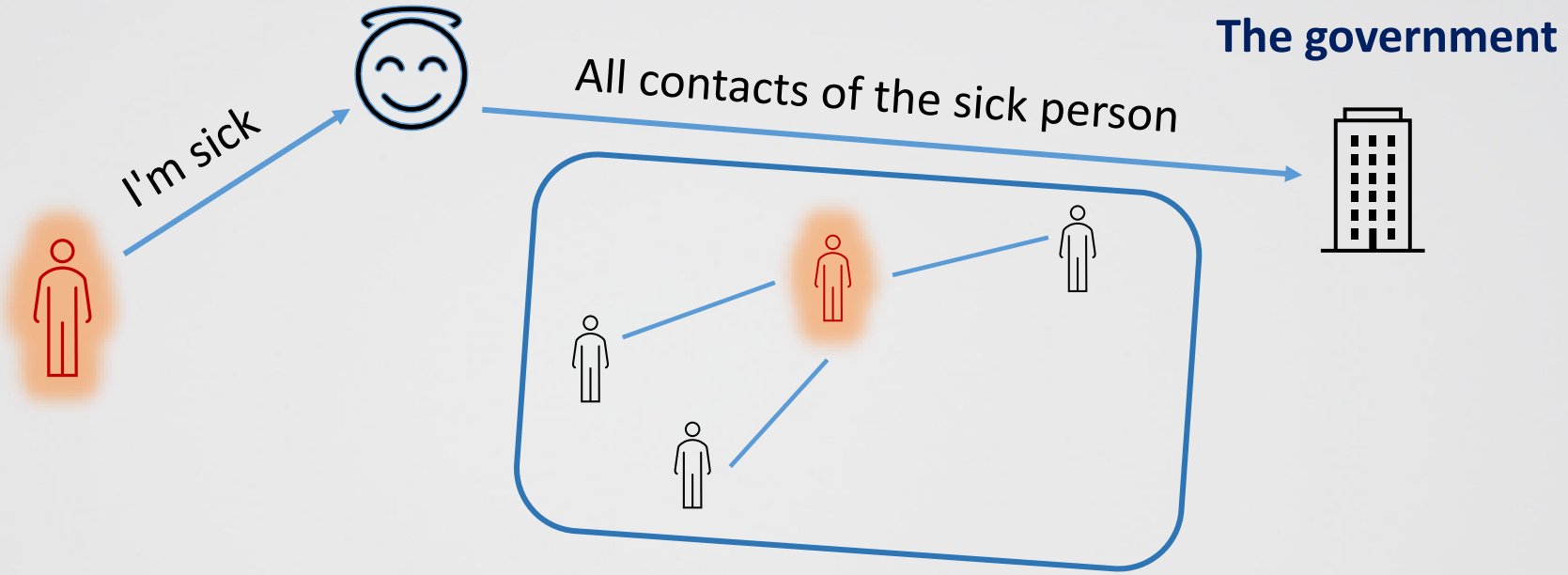
Knows all contacts (not necessarily locations)



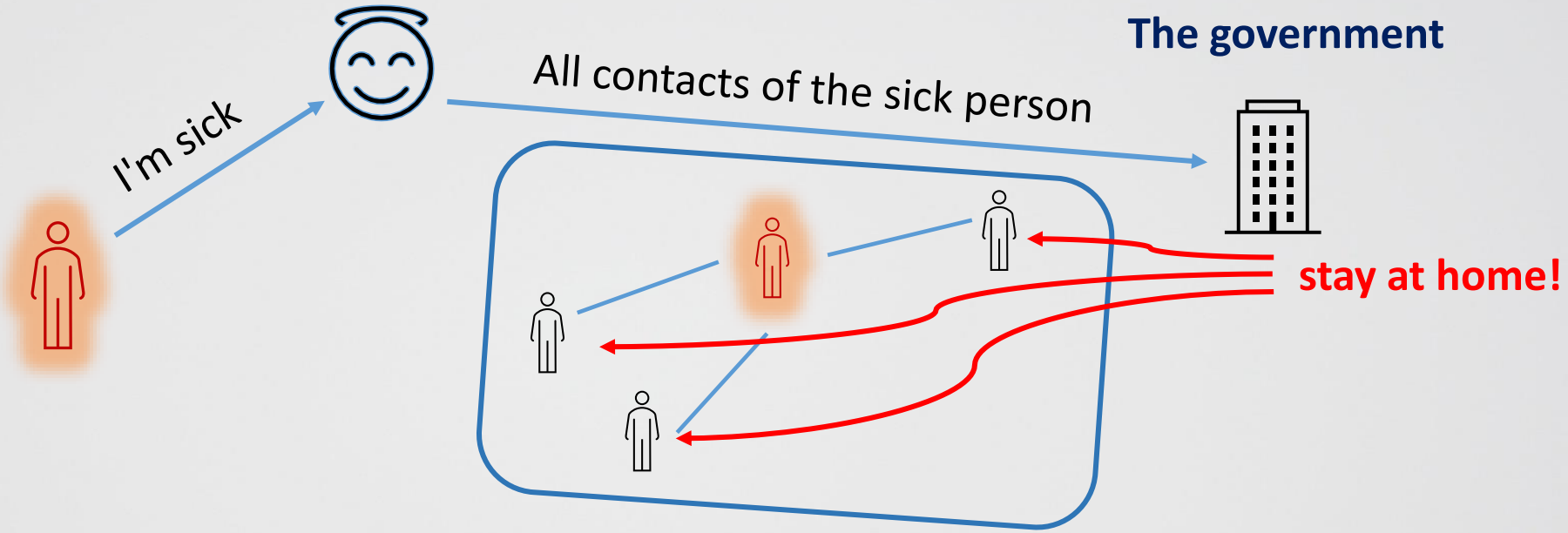
In an Ideal World



Centralized Output

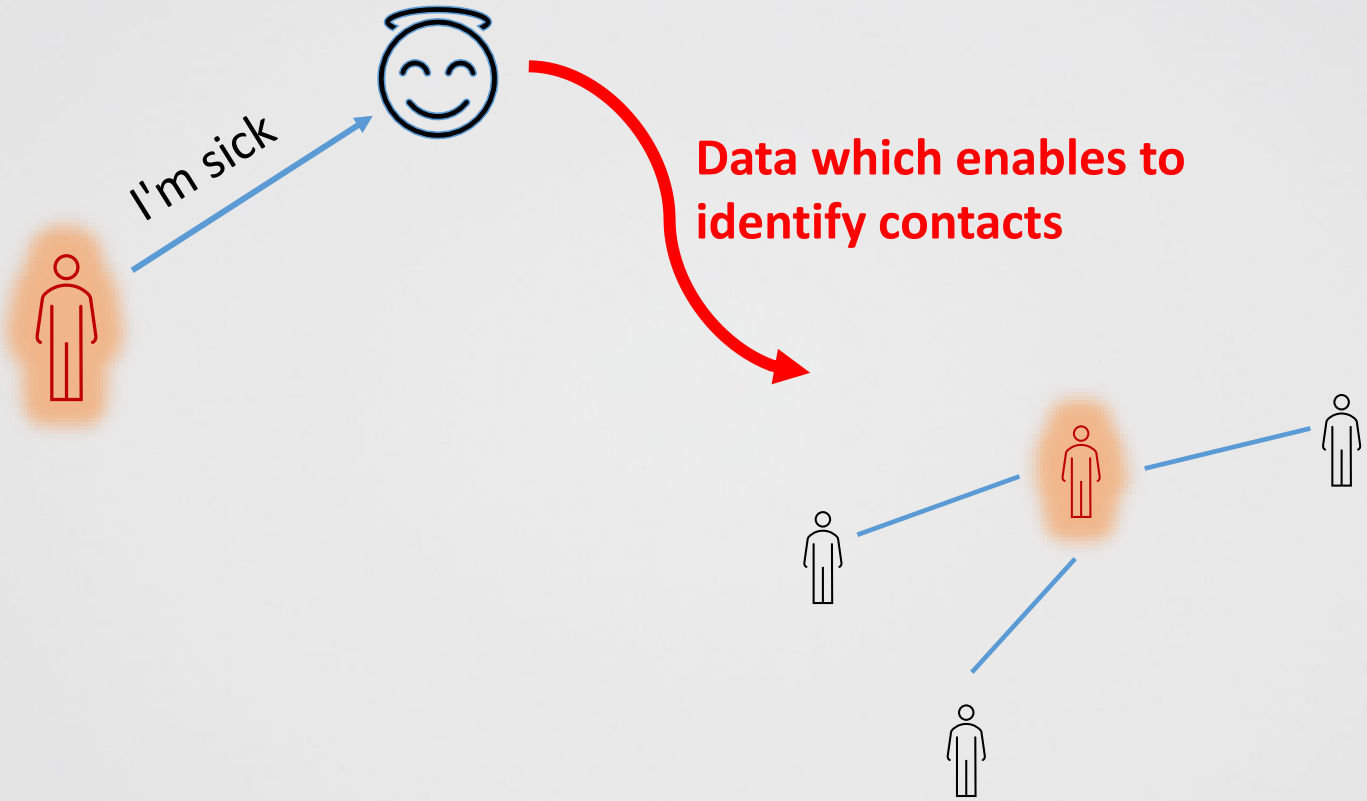


Centralized Output

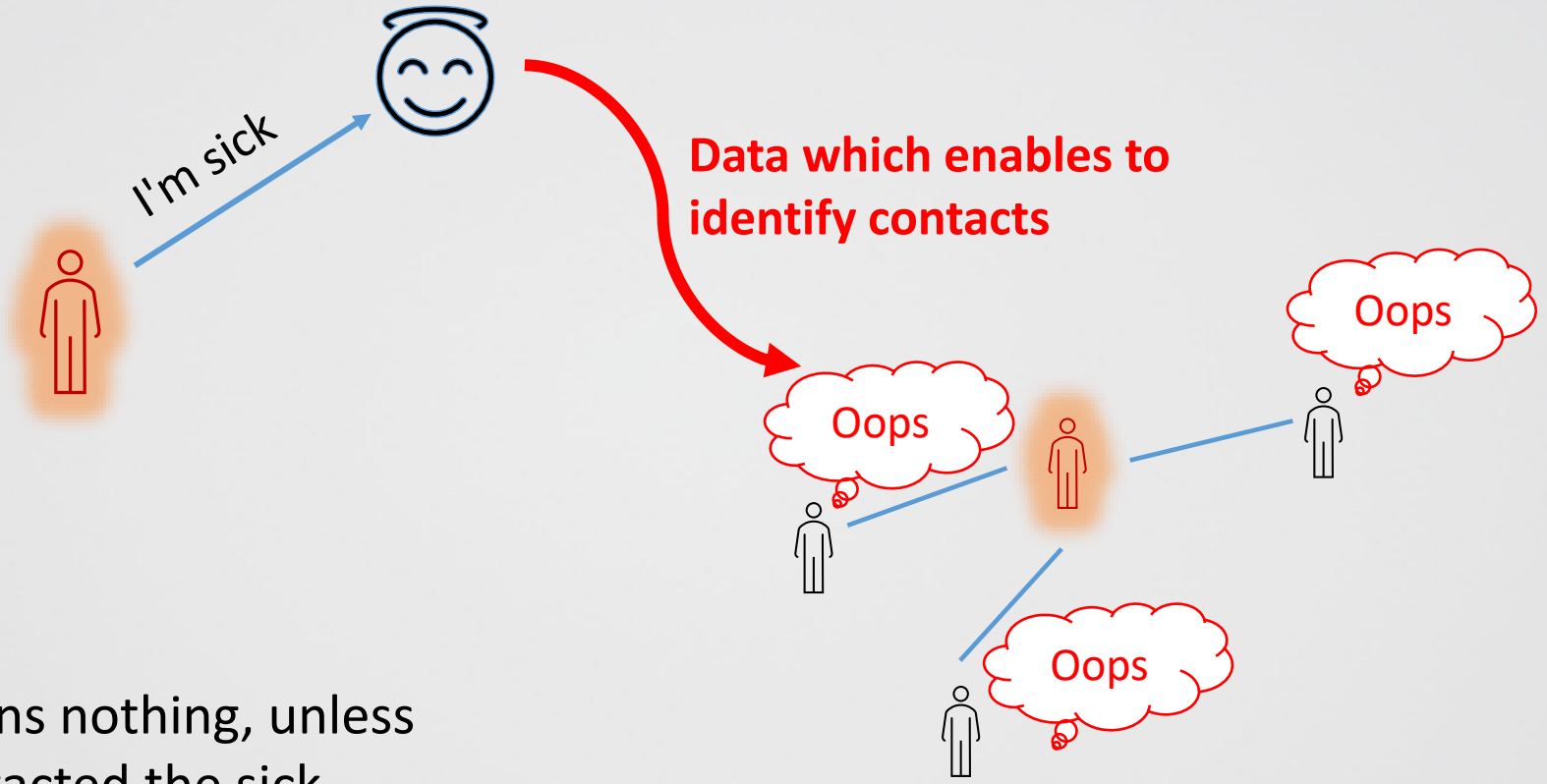


Government does not learn about
the contacts of non-infected people
(in this ideal implementation)

Decentralized Output

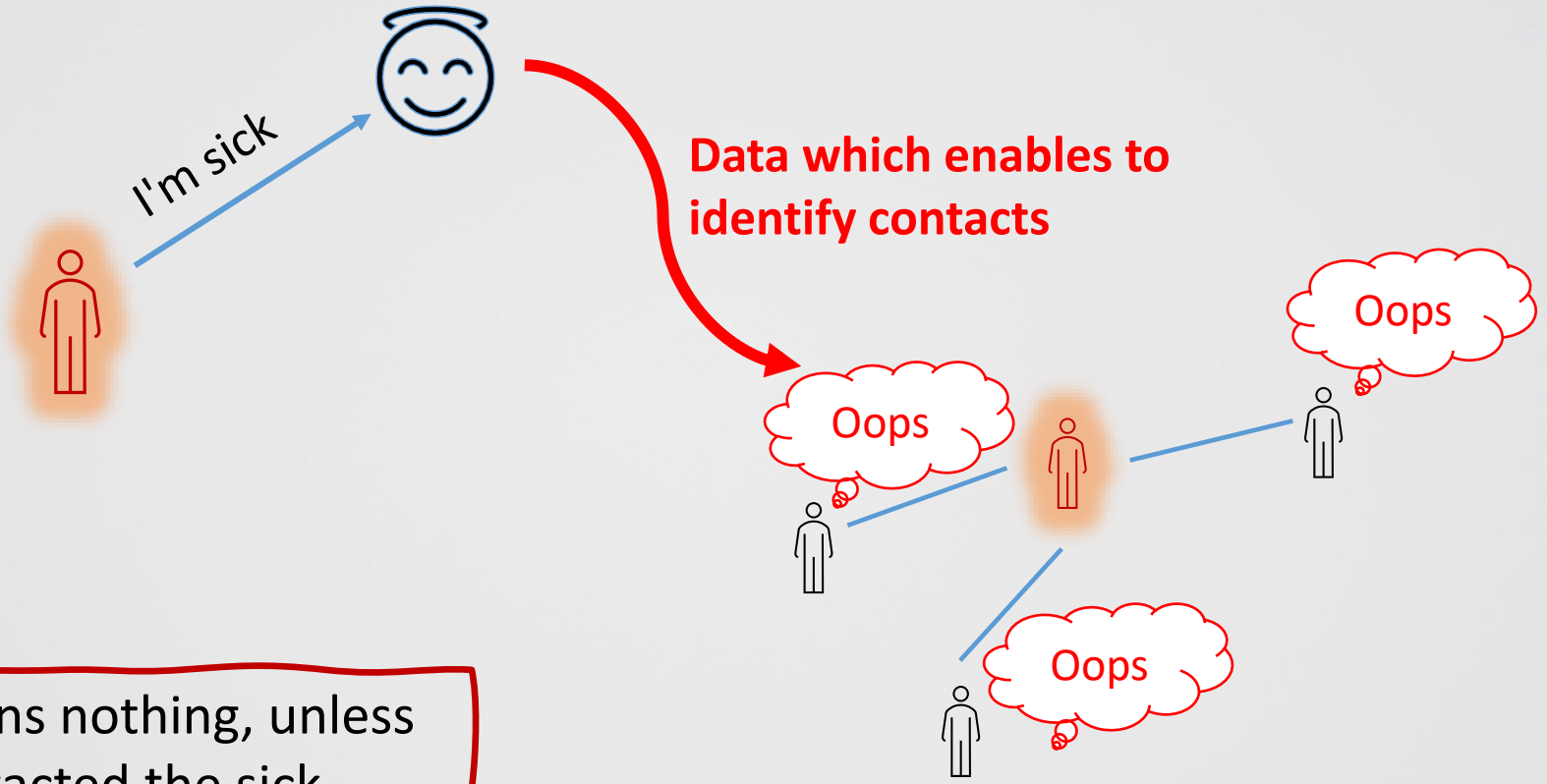


Decentralized Output



Government learns nothing, unless if those who contacted the sick person want to report about this

Decentralized Output



Government learns nothing, unless if those who contacted the sick person want to report about this

Centralized vs. Decentralized

- Who controls the data? (government vs. users)
- Who gets the output? (government vs. users)

- Centralized (Singapore, Australia): we must trust that the government does not misuse its power

- Decentralized (Europe / GAEN): we must trust that users will do the right thing

The Challenge

- Asian countries fought COVID-19 pretty well using centralized information

- Can western countries do well while keeping less information about people?

Our basic approach

- Users must trust that the system preserves their rights (privacy and accuracy)
- Otherwise they will “cheat”
- The government will then try to make the system stronger, but we don’t want to get there

Current Situation in Israel

- Rolled out a decentralized tracing app which is not based on GAEN
  - (because there were good reasons to also use location data)
- 40% of cellular users installed the app
  - Despite the lack of an effective media campaign
- But most of these users later uninstalled the app
  - Usability – battery usage
  - Loss of trust in the government

A Blueprint for Decentralized Contact Tracing

- Each user keeps a log of his whereabouts
- Sick users send these logs to the government
- The government broadcasts this information
- Others can check if they were infected

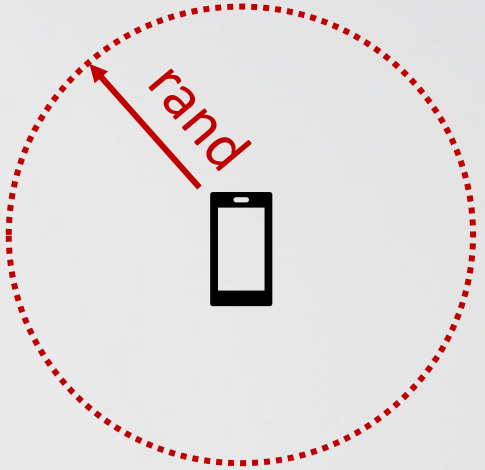
- GPS location (Hamagen 1)
- BLE (Hamagen 2)
- QR codes (future?)

A Blueprint for Decentralized Contact Tracing

- GPS location:
  - Inaccurate
- BLE:
  - More accurate
  - Requires support from Google/Apple, or special hardware
- QR codes:
  - Simple
  - Effective only for designated spaces
  - Requires user action

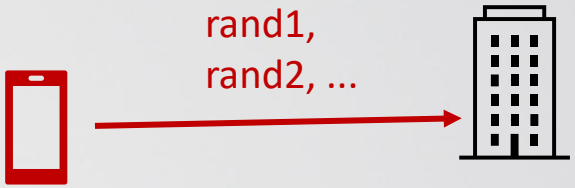
Basic decentralized design

- Every 5 minutes each device picks a random value and broadcasts it over BLE



Basic decentralized design

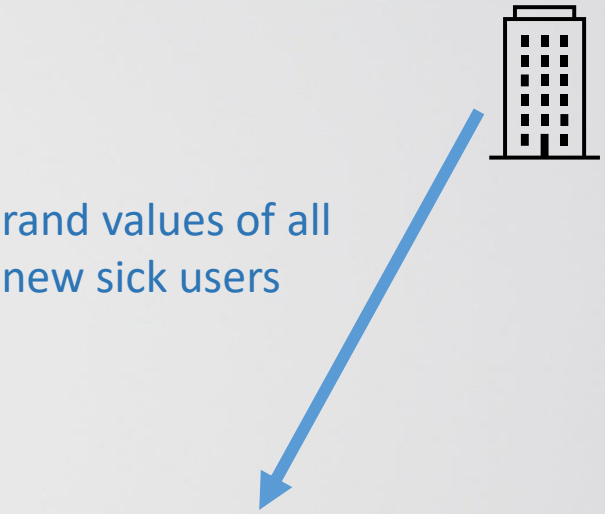
- Every 5 minutes each device picks a random value and broadcasts it over BLE



- If user is COVID positive, he can choose to give the government the list of values that he broadcasted

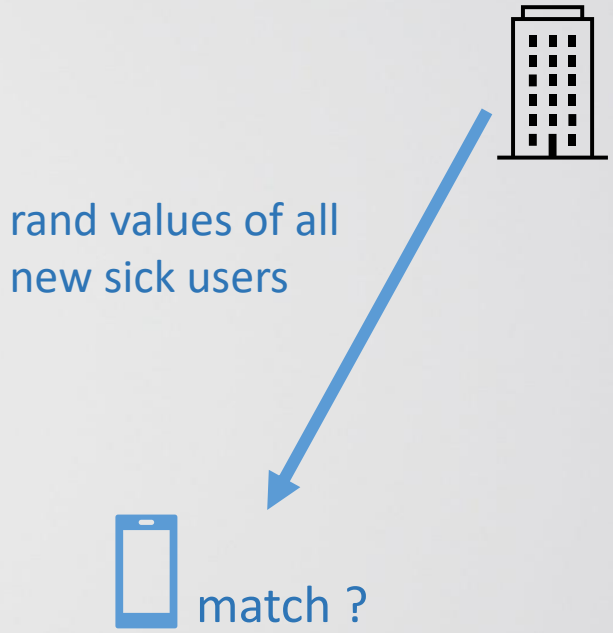
Basic decentralized design

- The government broadcasts the random values received from all new COVID+ people



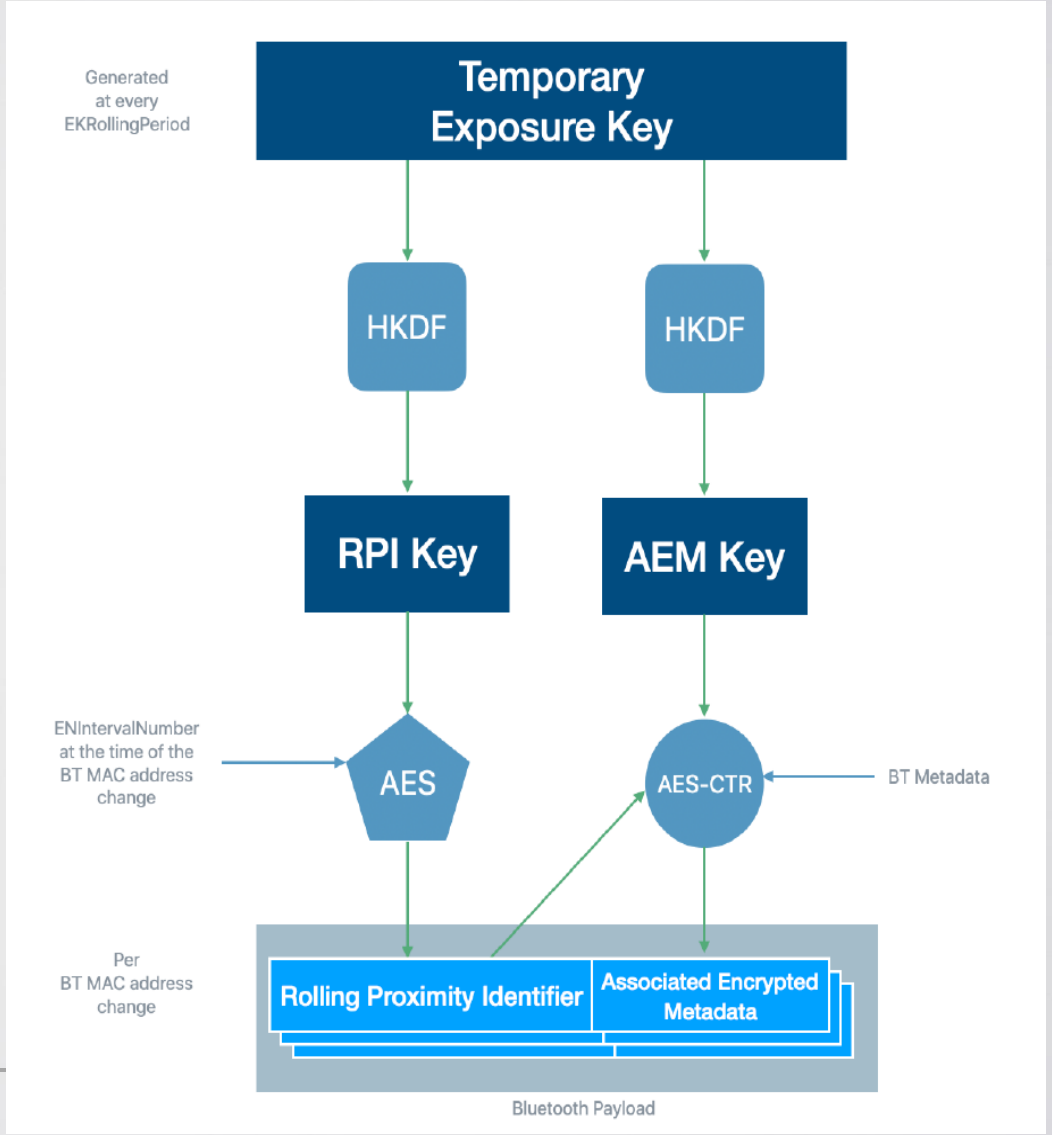
Basic decentralized design

- The government broadcasts the random values received from all new COVID+ people
- All users compare this list to the values that they received
- If there is a match then they can choose to report this



Google/Apple

- Android/iOS prevent applications from efficiently sending/receiving BLE messages
- Google/Apple suggest an API which is similar to the basic decentralized design
  - **Generate random key for each day**
  - ***All* BLE messages for the day are derived from a daily key**
  - **Infected person's daily "Temporary Exposure Keys" are broadcasted to all users**
- The companies prevent apps that use location data from using their API



My Interpretation of GAEN

- ``Perfect is the enemy of good''
  - *Dans ses écrits, un sage Italien*
    Dit que le mieux est l'ennemi du bien
- Wanted to deploy something quickly and widely

- Location data is a PR nightmare, so best avoid it
- Although they are only companies, they control the market and can effectively decide on the rules

Huge difference between countries

- Switzerland:
  - Must protect the identity of the COVID-19 positive person
  - Therefore the system only informs other people about the day in which they met that person

- Israel:
  - People would not believe the system if they are not convinced that they indeed met the sick person
  - Therefore must inform users about the exact time of exposure to COVID-19

Huge difference between countries

- Other issues in Israel:
  - It is likely that there will be attacks against the system (either by amateur hackers, or by malicious hackers)
  - People might claim that they were exposed to COVID-19 in order to gain something (students before exam?)
  - If people do not trust the system then they will cheat

Differences between our solution and GAEN

Tradeoff Between Privacy and Explainability

- GAEN only reveals the day of the contact
  - No “explainability”

- We suggest revealing location and coarse time of contact
  - To convince users that they were indeed exposed

Linkability and Partial Disclosure

- GAEN sends a single key per day
- Attackers can thus *link all IDs* that an infected person sent on the same day
- It is also impossible to redact "sensitive" time periods

- We suggest using **hourly keys** - prevent linking exposures in different hours
- Using a "**Tree**" like key derivation scheme to allow flexible tradeoff between privacy and communication complexity
- And allowing the user or MoH to **redact different periods of time**
- **Better privacy**

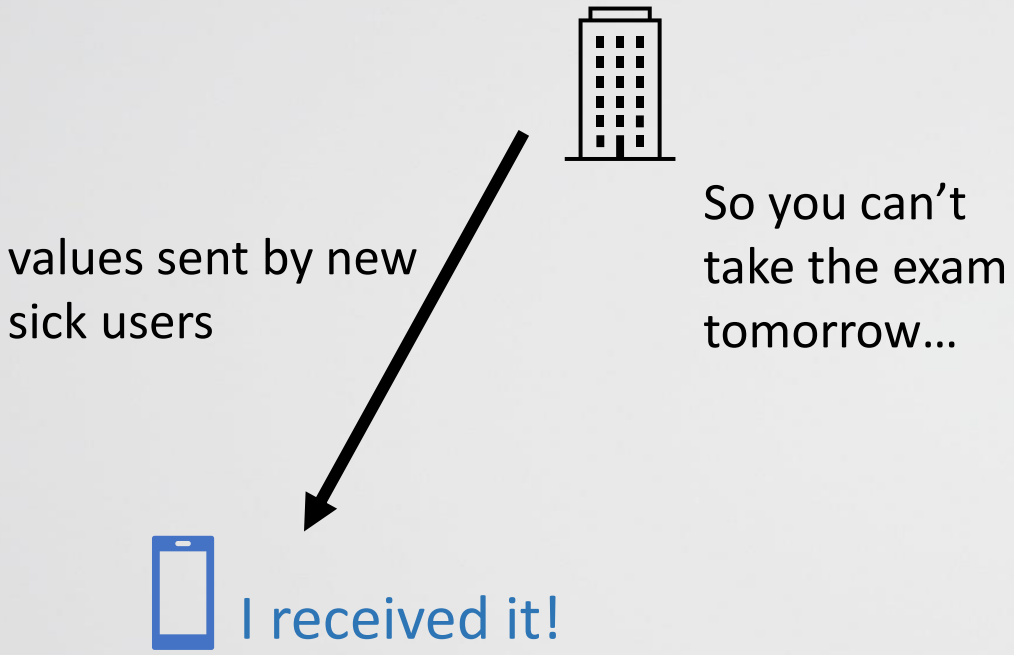
Relay Attacks

- Attack Scenario
  - BT receiver is placed in an emergency room
  - BT transmitter is placed in a busy supermarket

Protecting against Relay Attacks

- GAEN is insecure wrt these attacks
- We suggest sending the user's coarse grain geohash
  - Receiver anyway knows this location
  - Server does not learn the location
- Tradeoff between security and privacy
  - Location information stored on device might be compromised or subpoenaed
- More advanced attacks are still possible
  - e.g., colluding with an infected person

Proving exposure to COVID+

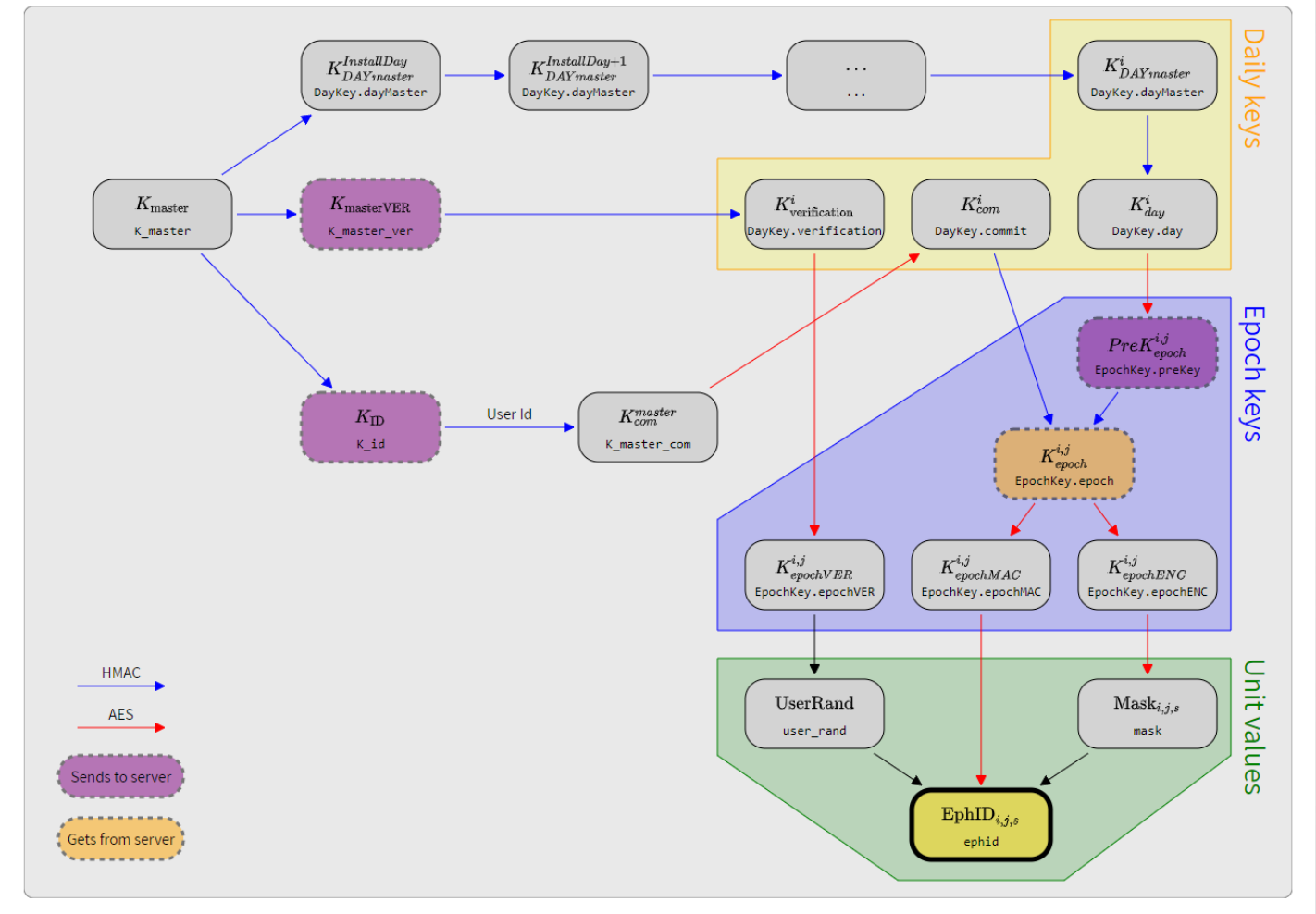


- In GAEN users can just claim that they were exposed to a patient
- Our design enables users to prove that they were exposed

How to prevent coercion?

- User choice is required for trust
- App usage must be voluntary
  - Users might still be coerced to install (e.g., by employers)
- Users should be given the option
  - To decide if a notification is correct or is a false positive
  - To choose whether to notify the authorities or not
  - To disable BT transmission and / or reception
  - To delete keys for specific time intervals
  - To delete notification history
- Otherwise, users will find ways to "cheat"
- Hopefully, most users will do the right thing

Our Key Derivation Scheme



Current Status

- Sending and receiving BLE messages *without* the GAEN API is hard
- Google/Apple required that no location data is used

- Israel decided that its app must use location data
  - Mostly for supporting users who do not have smart phones
  - And to support better security (no relay attacks)

Current Status

- The application failed – people do not use it
- The app could be better: battery usage
- Many trust issues
  - Is the government going to track everything I do on my phone?
  - Too many new patients (not anymore), so why should I bother doing anything?
  - Insufficient campaign
  - Government happy with secret service solution

What is the most important thing can we do?