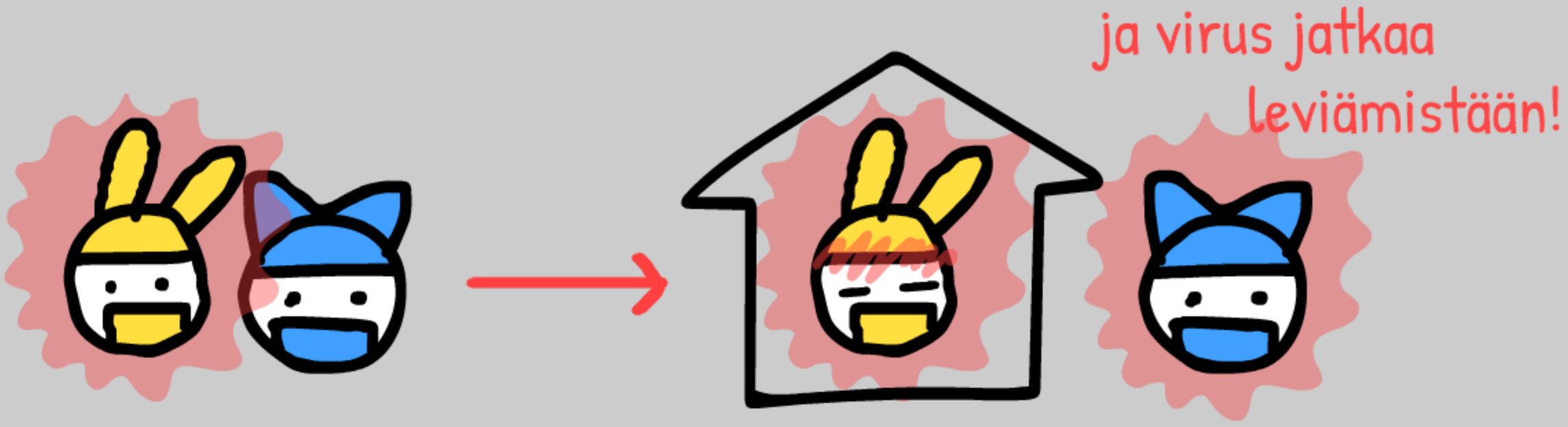
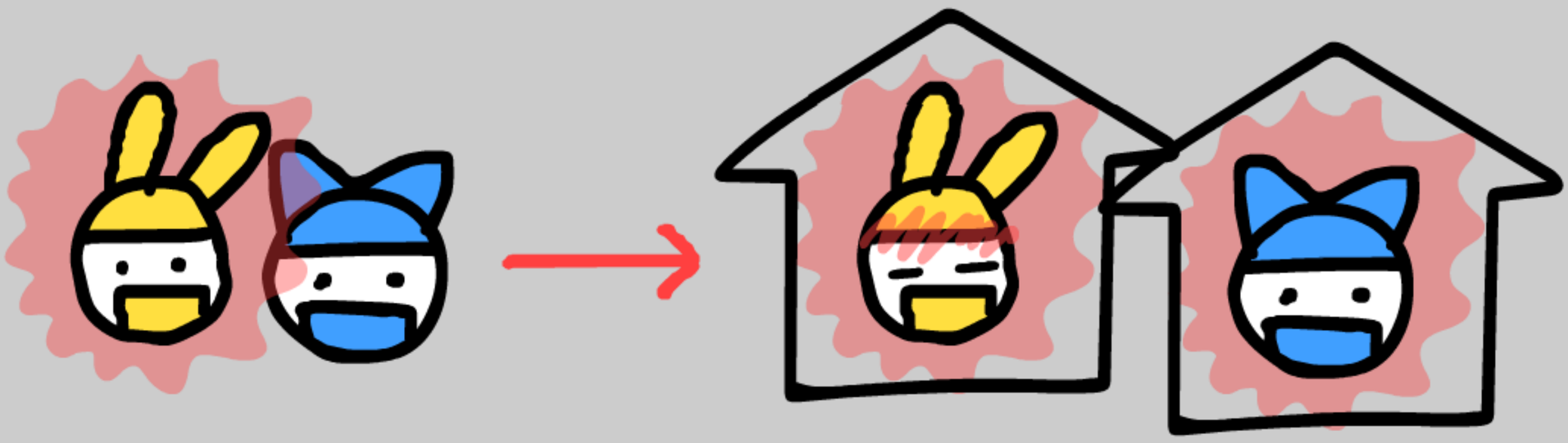
TURVATAAN TERVEYS & YKSITYISYYS

Koronan (eli COVID-19) kanssa
ongelma on se, että olet
tartuttaja jo noin kaksi päivää,
ennenkuin tiedät olevasi saanut tartunnan.



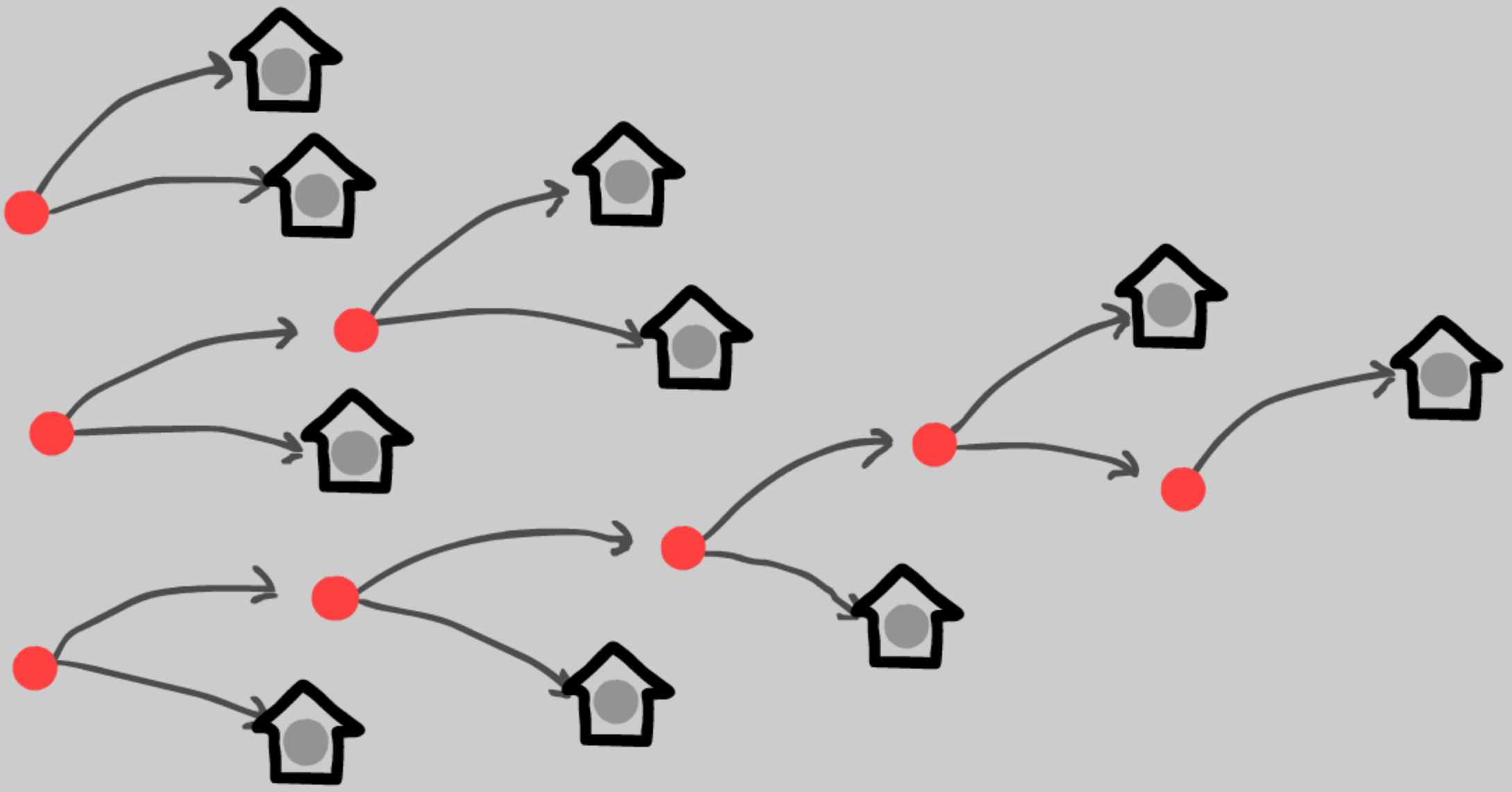
Kestää kuitenkin noin 3 päivää ennnenkuin
sinusta tulee tartuttaja. Jos osaisit
hakeutua karanteeniin samana päivänä,
kun saat tarunnan...



...pysäytämme viruksen leviämisen
olemalla askelen edellä!

*entäs täysin oireettomat levittäjät? He eivät itse asiassa ole kovin-
kaan suuressa roolissa viruksen leviämisessä, kts. viitteet lopussa.

Tätä kutsutaan "kontaktien jälji-tykseksi". Samaa tekniikkaa käyt-tävät esim. Etelä-Korea ja Taiwan jo nyt koronan kurissa pitämiseksi. Meidän olisi syytä tehdä samoin.



Eikä meidän tarvitse ihan kaikkia kontakteja edes löytää! Tarvitaan vain noin 60% niistä...

*miksi noin 60%? Katso viitteet lopusta!

...Mutta meidän täytyy löytää kontaktit nopeasti. Perinteinen kontaktien jäljittäminen haastatteluin on liian hidasta.

Siksi tarvitsemme kontaktien jäljitys-sovelluksen.

Mutta joudummeko luopumaan yksi-tyisyydestämme terveytemme varjolla?

NO

E!!

On ihan mahdollista samalla
sekä turvata terveys että
huolehtia yksityisyydestä melko
yksinkertaisella tavalla!

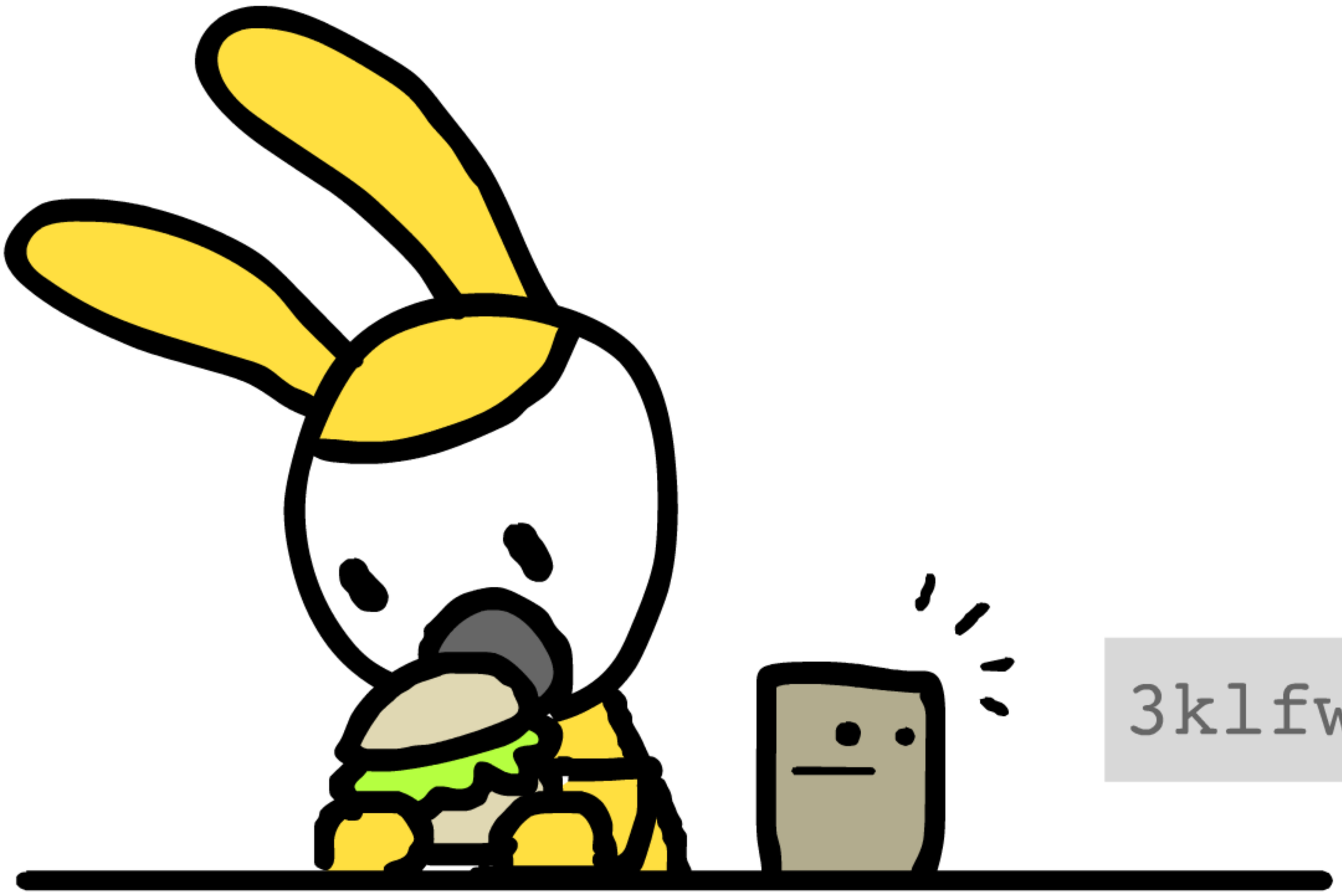
Katsotaanpa kuinka se toimii
Sannan ja Timon avulla...

Sanna lataa jäljityssovelluksen.
(Sen lähdekoodi on avointa, joten ihmiset pystyvät tarkistamaan, että se todellakin toimii oikein...)

Kerran viidessä minuutissa hänen puhelimensa lähettää tiettyjä satunnaisia merkkijonoja muille lähialueen laitteille Bluetoothin kautta.

* 5 minuuttia on vain esimerkki! Teknisesti viestin lähettely on puolittain satunnaista. Mutta sillä ei ole kauheasti väliä.

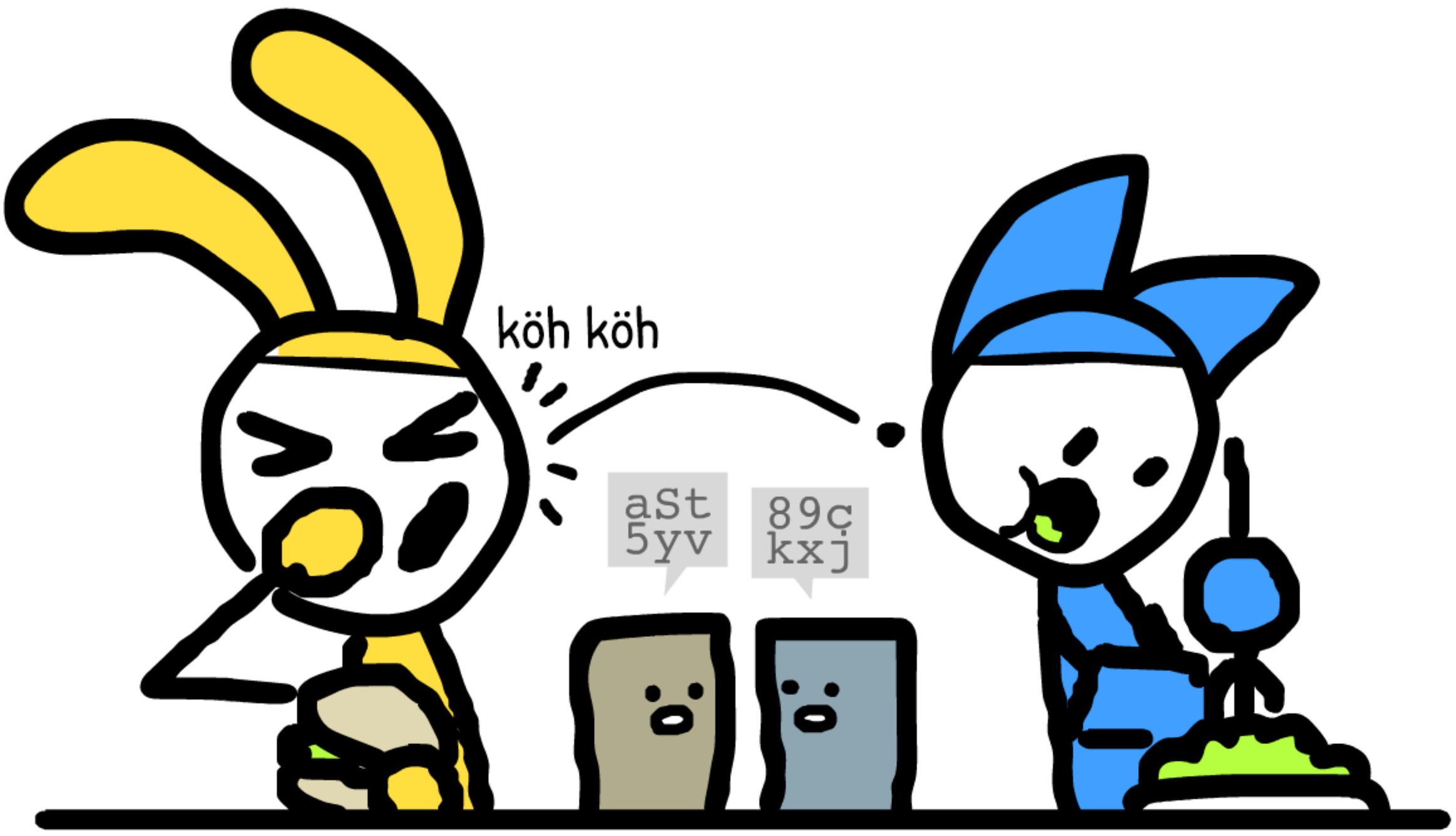
Koska viestit ovat satunnaisia, eikä GPS-paikannusta käytetä, viesteihin ei sisälly mitään henkilökohtaisia tietoja, kuten identiteettiä tai sijaintia.



Samalla, kun hänen puhelimensa lähettää satunnaisia viestejä, se myös kuuntelee vastaavia viestejä lähellä olevista puhelimista.

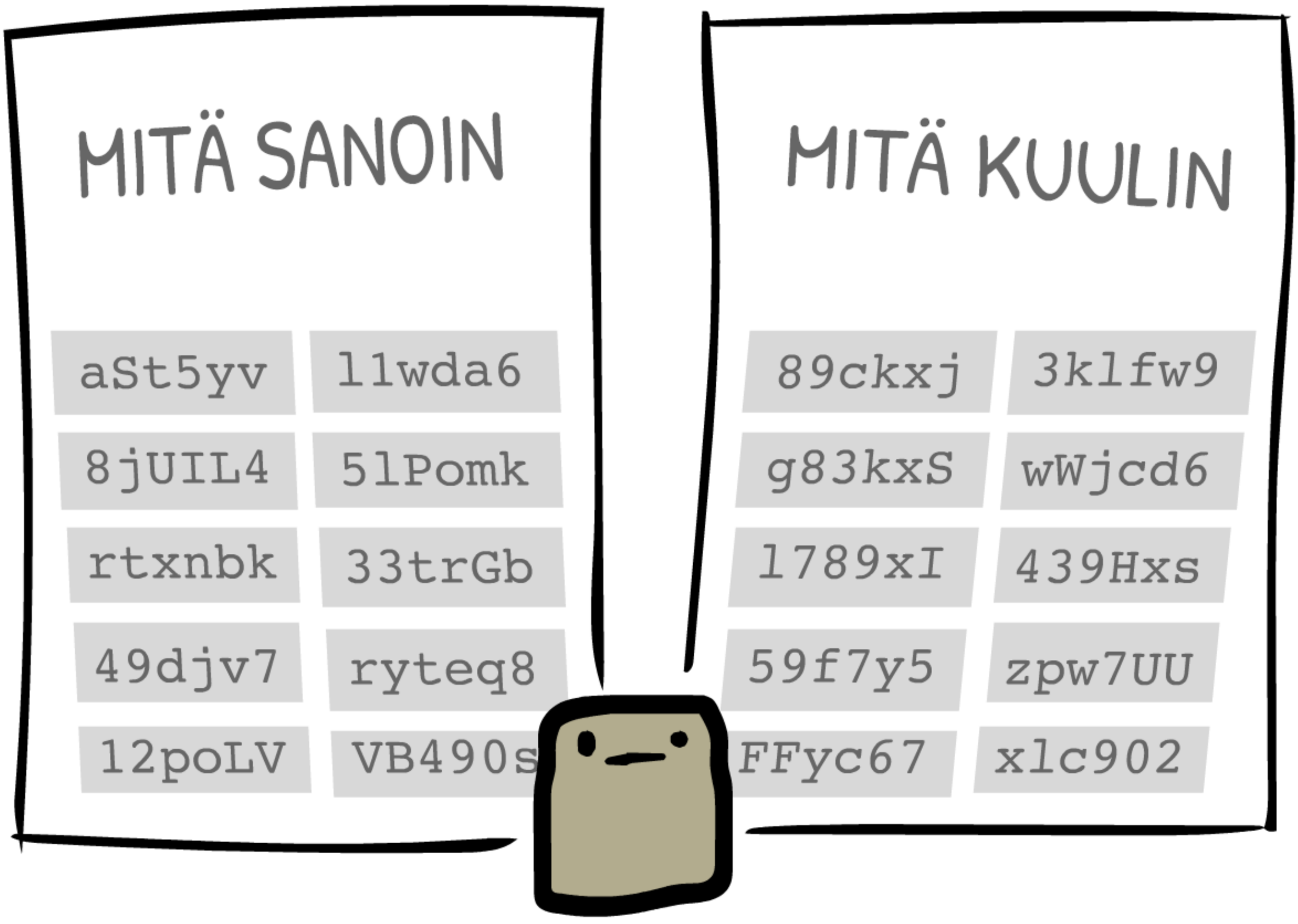
...esimerkiksi Timolta.

Timolla on yksityisyyttä kunnioittava jäljityssovellus, joka on yhteensopiva (tai sama) kuin Sannalla.



Jos Sanna ja Timo sattuvat olemaan reilut viisi minuuttia lähekkäin, heidän puhelimensa vaihtavat ainutkertaisia viestejä.

Molempien puhelimet muistavat kaikki viestit, jotka ne ovat lähettäneet ja vastaanottaneet viimeisten 14 vuorokauden aikana.



Ja koska satunnaiset viestit eivät sisällä mitään tietoja Sannasta eikä Timosta, heidän yksityisyytensä säilyy turvassa!

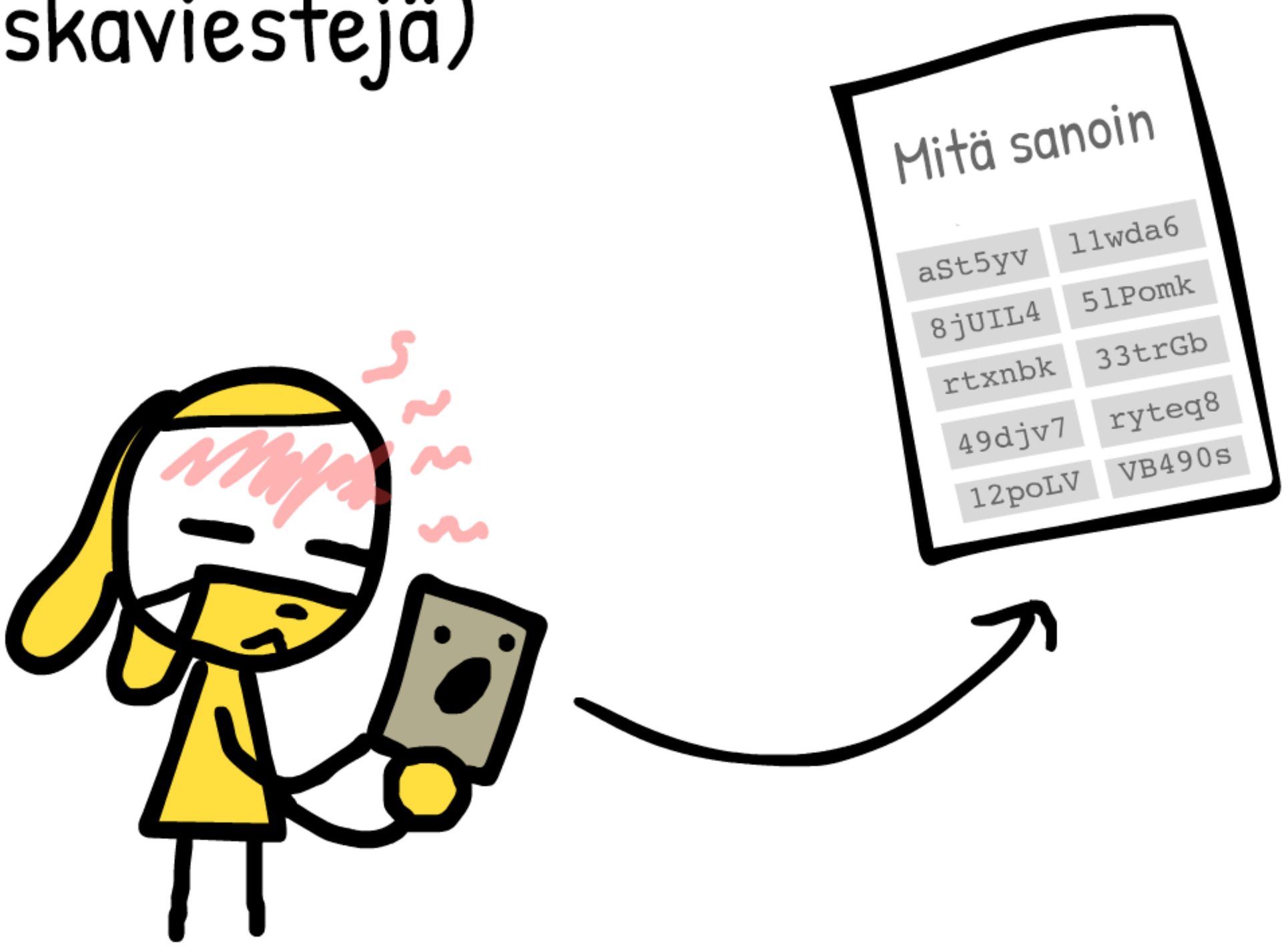
* 14 päivää on vain esimerkki! Voi olla, että epidemologit tarkentavat näkemystään tartuna-ajasta suuntaan tai toiseen.

Seuraavana päivänä Sannalle puhkeaa kuiva yskä ja kuume nousee.

Hänet testataan.

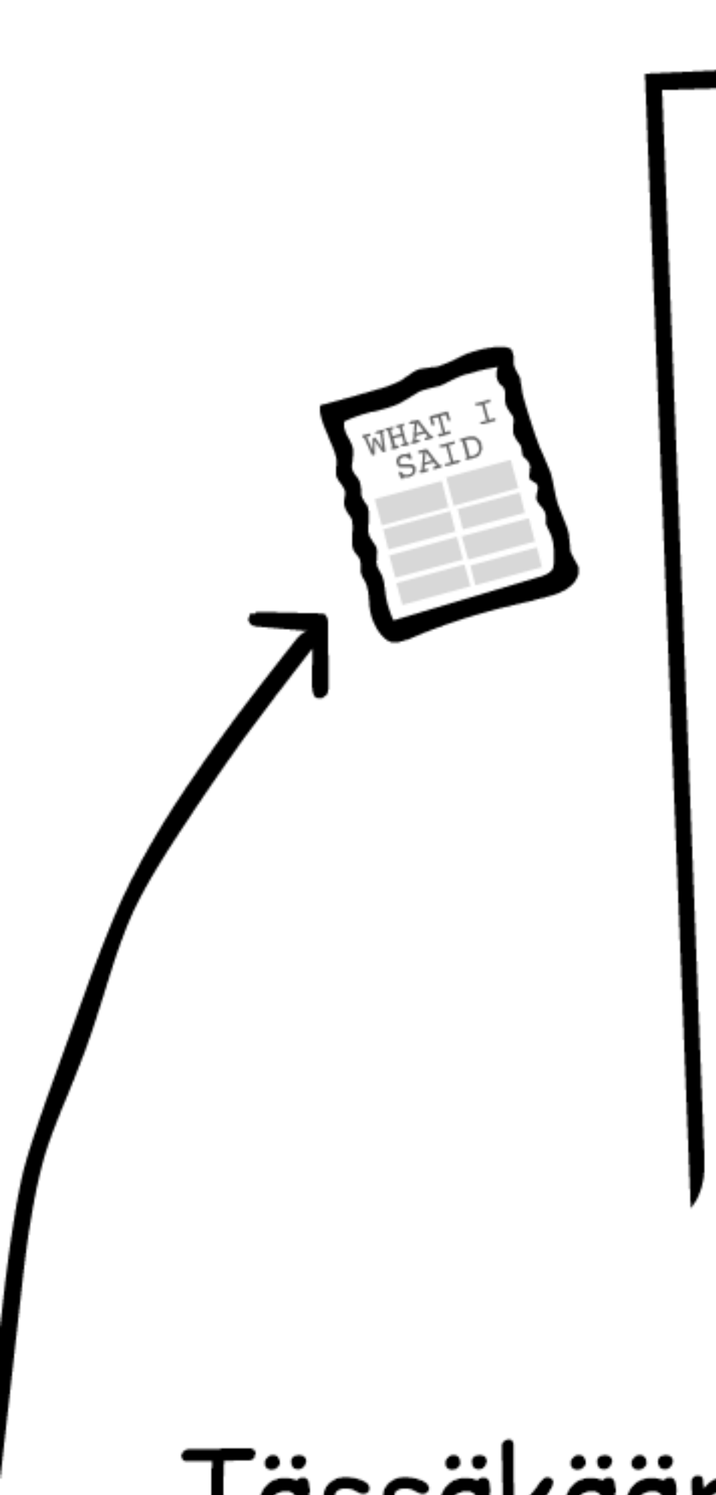
Sannalla on koronavirus.
Kerrassaan huono päivä hänelle.

Mutta hän ei aio kärsiä aivan suotta!
Sanna lähettää puhelimensa
"mitä sanoin"-viestit sairaalan
tietokantaan käyttäen kertakäyttöistä
salasanaa, jonka sai lääkäriltään.
(Salasana auttaa vähentämään
roskaviestejä)



Sanna voi halutessaan piilottaa osan
viesteistä sellaisilta ajankohdilta,
joita hän ei halua lähettää.

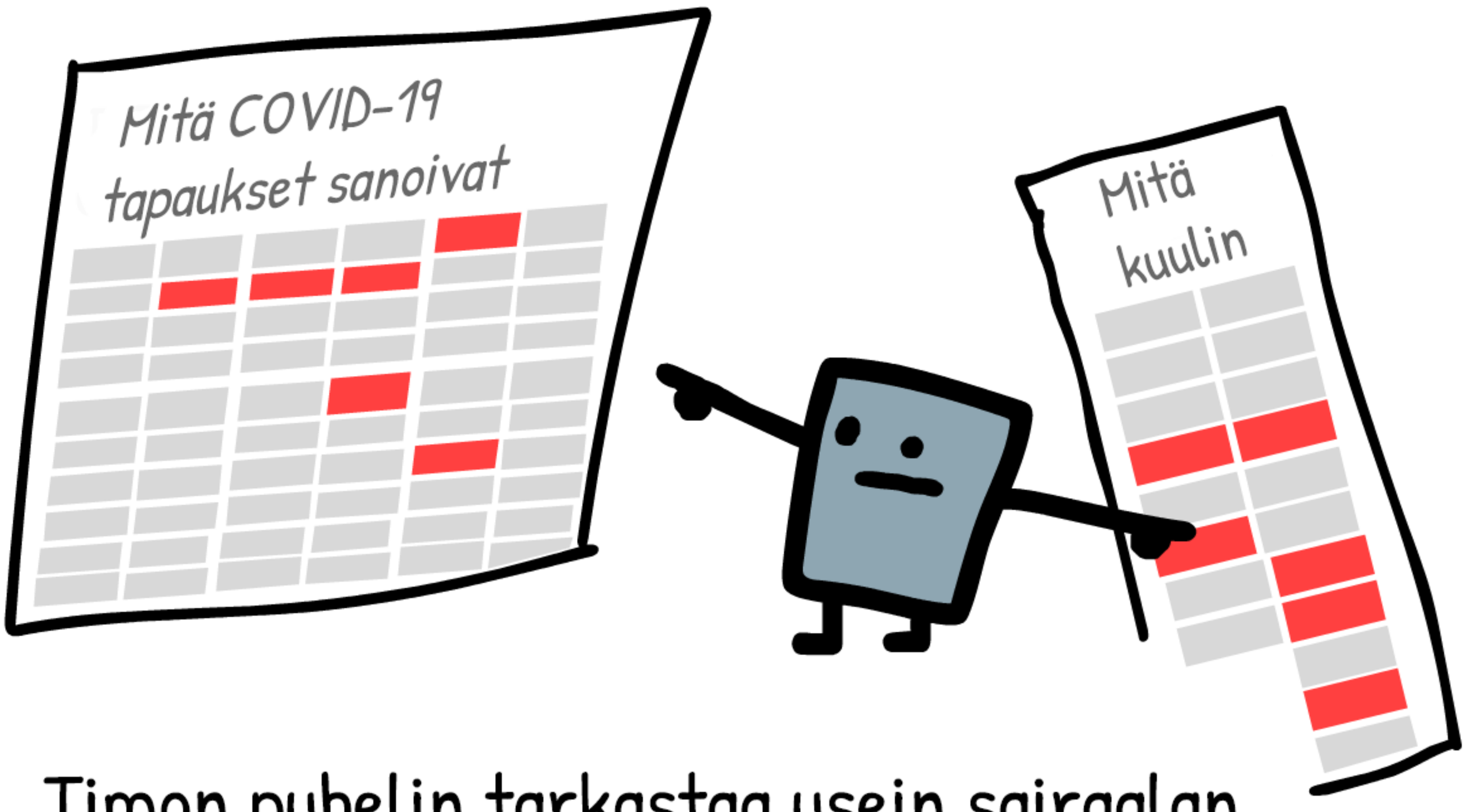
Sannan satunnaiset tekstinpätkät tallennetaan tietokantaan:



Tässäkään tilanteessa sekalaiset viestit eivät paljasta Sannasta mitään tietoja, esimerkiksi että kuka hän on, missä hän oli, kenen kanssa hän oli, mitä he olivat tekemässä, eikä sitä, kuinka monta ihmistä Sanna ylipäätään tapasi. Se ei ole tarpeen sairaalan näkökulmasta...

* jopa eri valtioiden sairaalat voivat vaihtaa viestejä keskenään, ja koska ihmisten tietoja ei välitetä, yksityisyys on turvattu.

...toisin kuin Timolle!

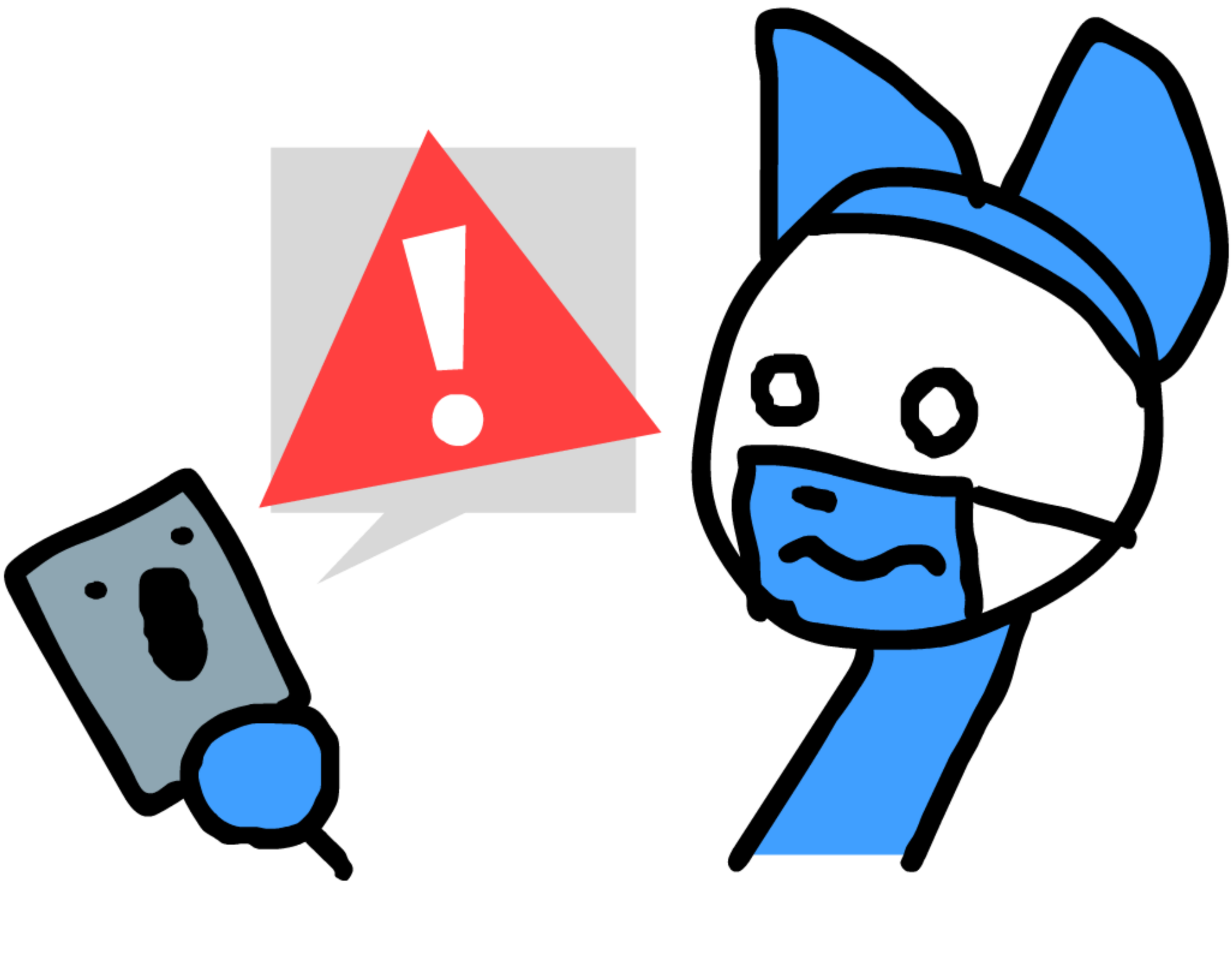


Timon puhelin tarkastaa usein sairaalan listan satunnaisista viesteistä, jotka on saatu korona-potilaiden puhelimista. Se etsii, josko se olisi "kuullut" jonkin näistä viesteistä lähellään olevista laitteista viimeisten 14 vuorokauden ajalta.

(Viestien satunnainen sisältö ei paljasta MITÄÄN HENKILÖKOHTAISIA TIETOJA)

* todellinen DP-3T protokolla on tätäkin turvallisempi. Se käyttää suodatusta, joka valitsee pelkät ne COVID-19 viestit, jotka Timon puhelin on kuullut - ei sairaalan koko tietokannan kaikkia viestejä

Jos se "kuuli", sanotaan vaikka kuusi tai enemmän viestejä COVID-19-tapaukselta (6 x 5 min = 30 min kokonaisuudessaan), se varoittaa, että Timon olisi syytä jäädä karanteeniin.

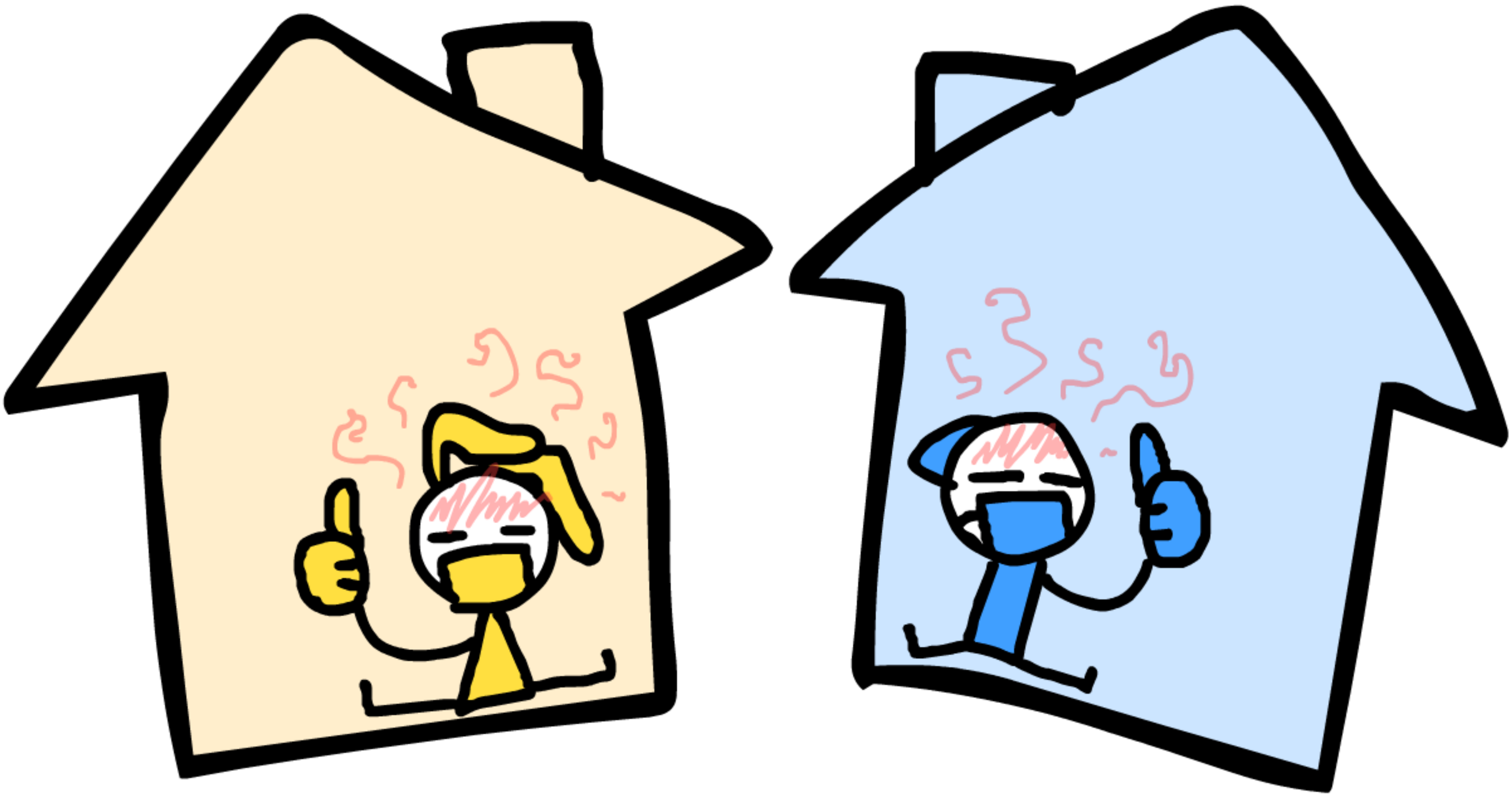


Näin Timo osaa katkaista tartuntaketjun - askeleen virusta edellä!

* huomaa, että luvut ovat vain esimerkkejä!

Tässä kaikki!

Tällä tavoin digitaalinen kontaktien jäljitys voi rajoittaa koronaviruksen leviämistä ennaltaehkäisevästi pitäen samalla yksityisyytesi suojattuna.



Kiitoksia Sanna ja Timo!
Pysykää turvassa!

LÄHTEET:

Tämä sarjakuva on karkea tiivistelmä **DP-3T** protokollasta 9.4.2020. Se on todellisuudessa paljon monimutkaisempi ja myös tietoturvallisempi, kts.

github.com/DP-3T/documents

On olemassa myös toinen vastaava yksityisyyden turvaava systeemi nimeltään **TCN Protocol**, kts.

github.com/TCNCoalition/TCN

Ja lopuksi täältä löytyy Oxfordin yliopiston tutkimus, joka perustelee, miksi kontaktien jäljityssovelluksilla voitaisiin välttää paikkojen sulkemiset:

Ferretti & Wymant et al. "Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing." *Science* (2020).

Tämä sarjakuva on

JULKISTA OMAISUUTTA

Se tarkoittaa, että voit saman tien lisätä sen uutissivuillesi. Ja olisihan se aika hienoa, jos laittaisit sen mukaan omaan kontaktien jäljityssovellukseesi! (Toki sillä varauksella, että sovelluksesi ihan oikeasti hyödyntää yksityisyyttä suojaavaa protokollaa)

Sinulla on myös lupa kääntää tämä toiselle kielelle! Käytetyt fontit ovat “Patrick Hand” sekä “Open Sans”)

Suomenkielinen käännös: Salu Ylirisku/Aalto-yliopisto

by **Nicky Case**
ncase.me + patreon.com/ncase

with huge help from
Prof. Carmela Troncoso (security)
& **Prof. Marcel Salathé** (epidemiology)