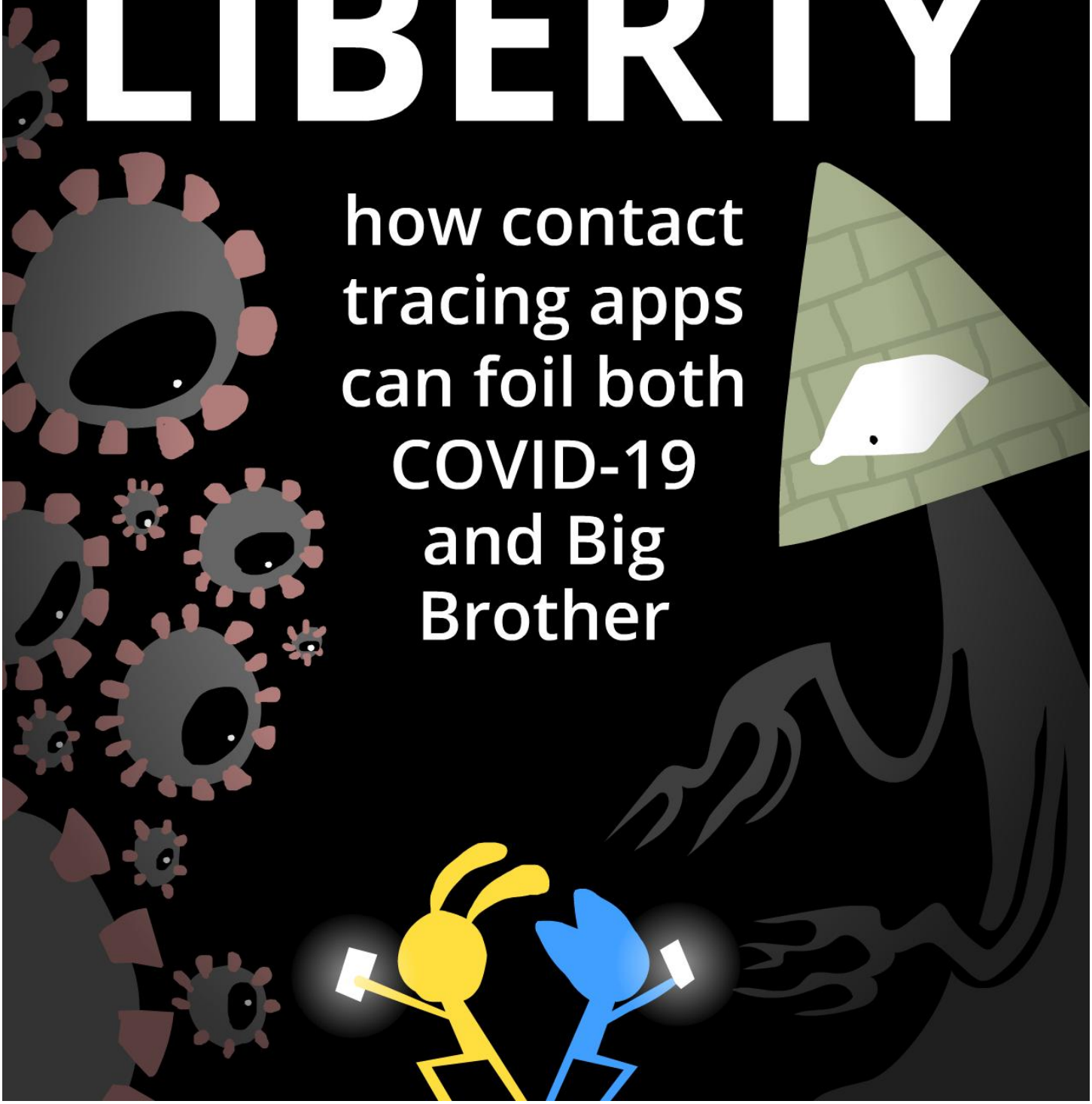
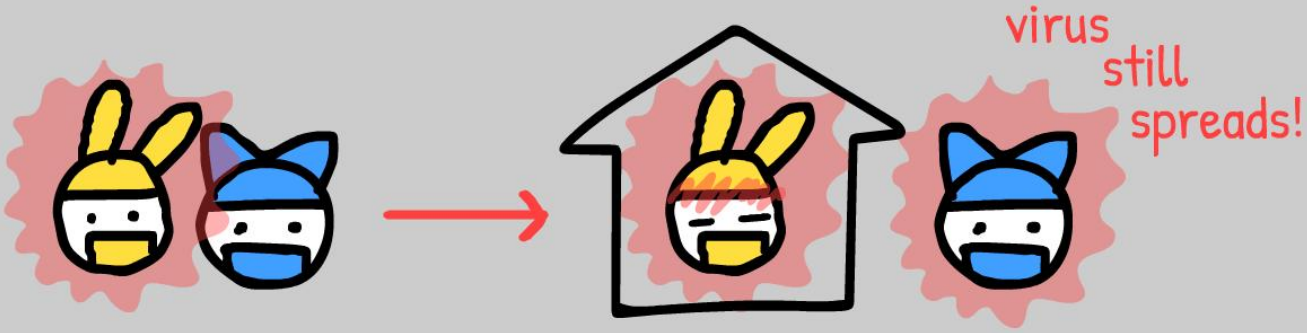
PROTECTING LIVES & LIBERTY

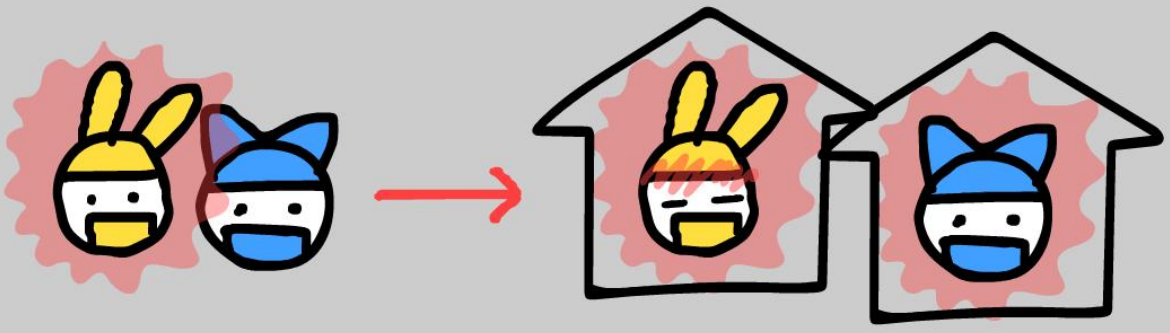
how contact tracing apps can foil both COVID-19 and Big Brother



A problem with COVID-19:
You're contagious ~2 days
before you know you're infected.



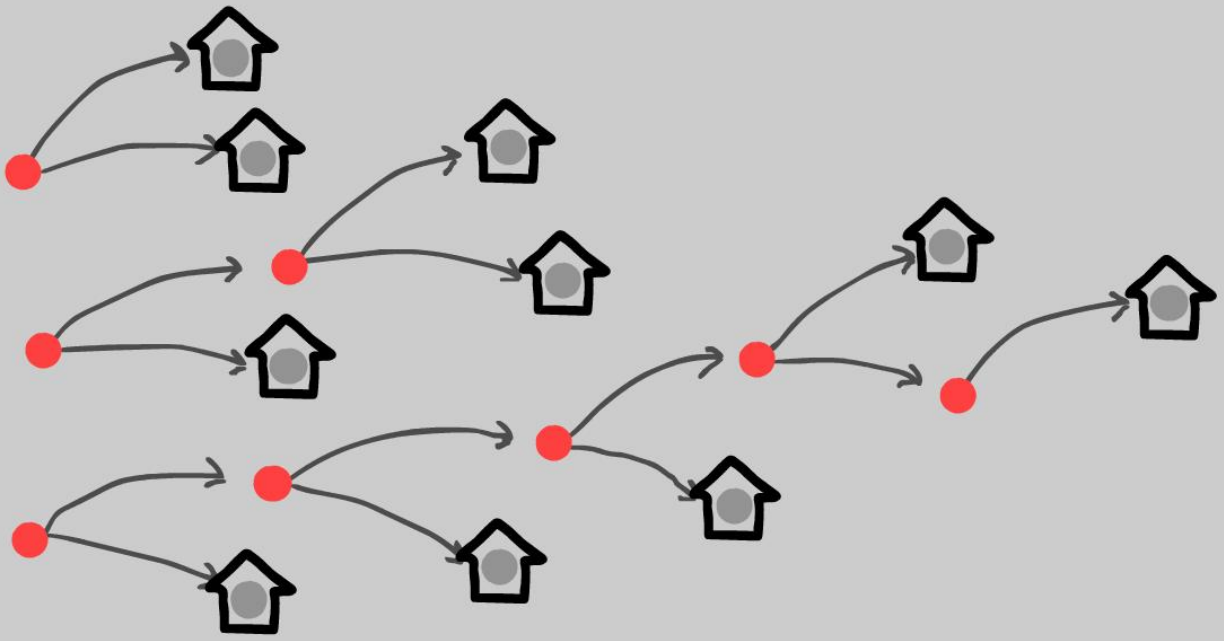
But it takes ~3 days to *become* contagious, so if we quarantine folks exposed to you the *day* you know you're infected...



We stop the spread, by
staying one step ahead!

* what about *never*-symptomatic people? turns out they don't play a large role in COVID-19 spread! see citations at end

This is called "contact tracing". It's a core part of how South Korea & Taiwan are *already* containing COVID-19, and what we must do, too.



We wouldn't even need to find all the contacts! We only need to find ~60% of them...

* ~60%? again, see citations at the end!

...but we *do* need to find them quickly. Traditional contact tracing, with interviews, is too slow.

Hence, why we need contact tracing *apps.*

But do we have to sacrifice privacy for health?

HECK
NO!

It's entirely possible to protect peoples' lives AND liberties, with a really simple process!

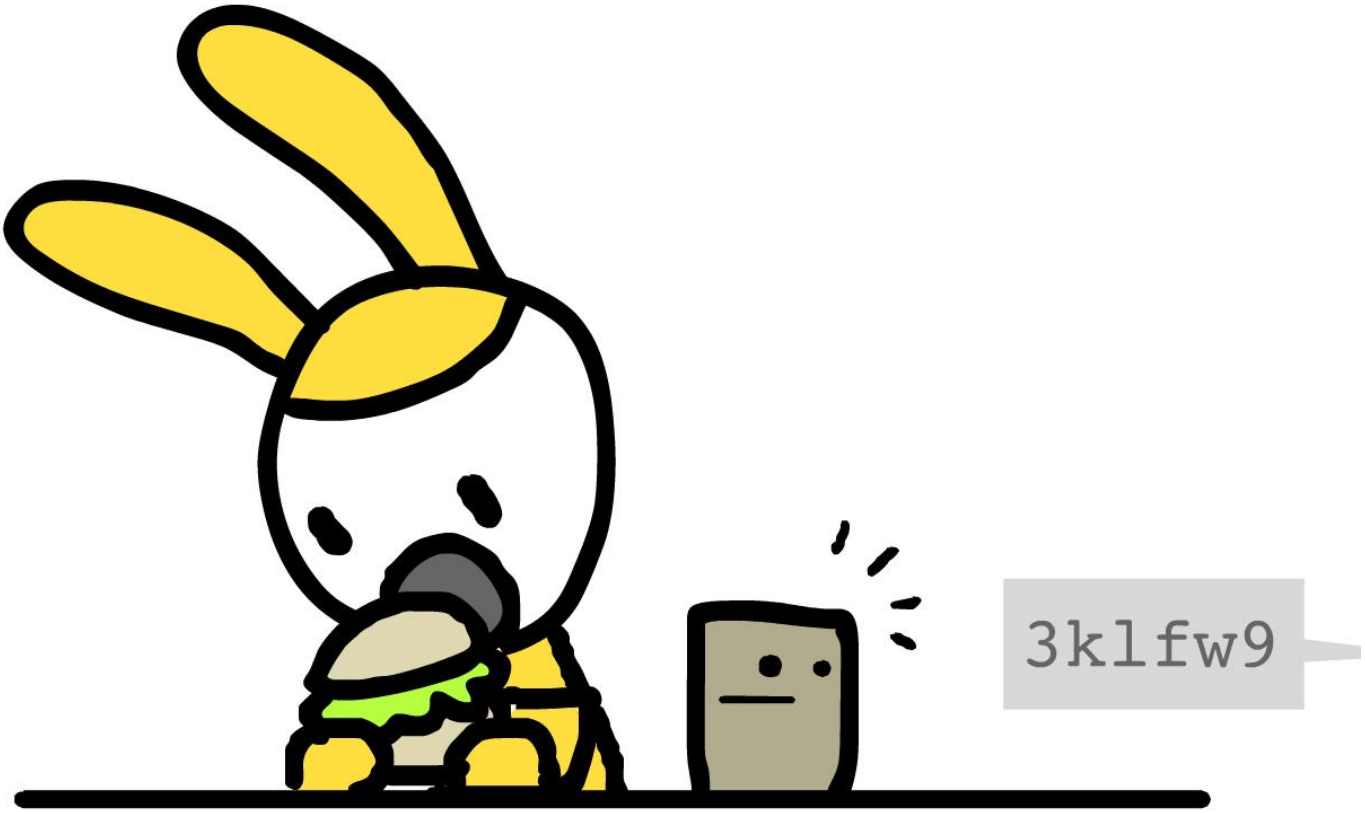
Let's see how it works, with the help of Alice & Bob...

Alice gets a tracing app!
(& its code is open to the public, so folks can verify it in fact does the following...)

Every 5 minutes, her phone says uniquely random gibberish to all nearby devices, using Bluetooth.

* 5 minutes is just an example! and technically it's "pseudo-random," since it's not quantum... does NOT matter.

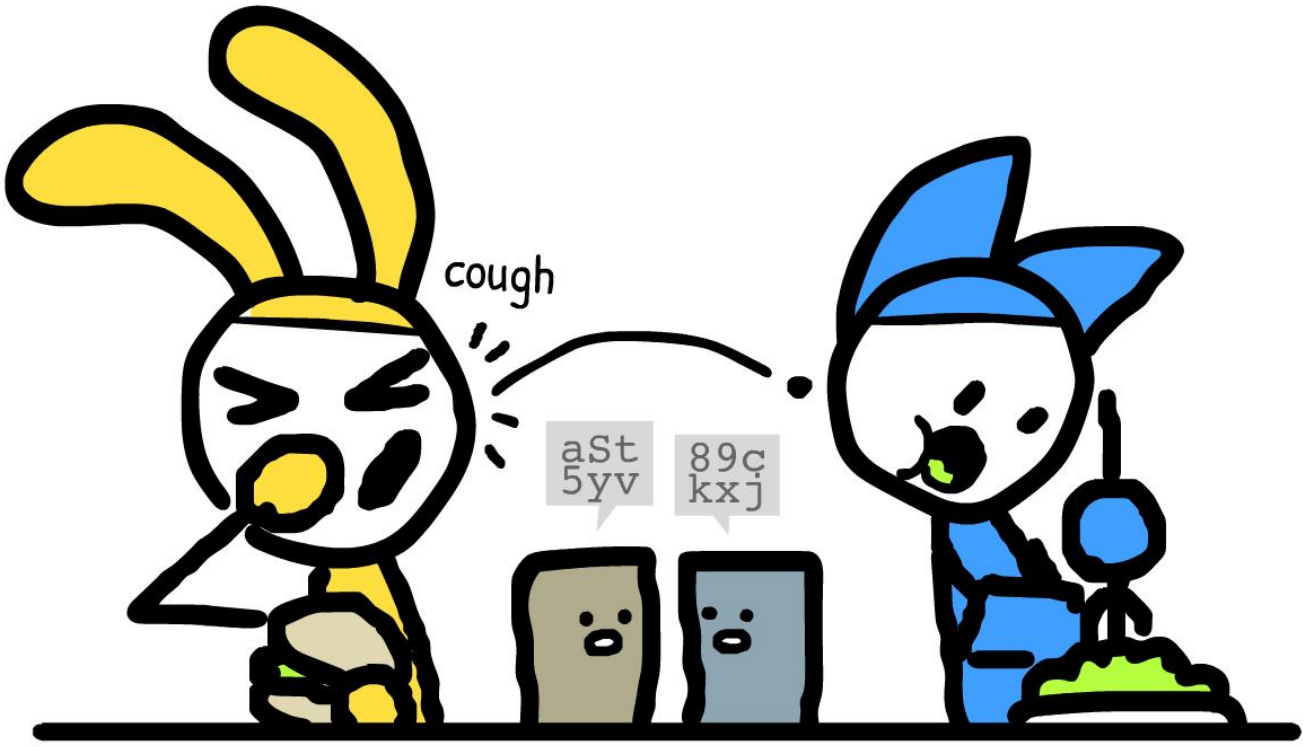
Because the messages are random & don't use GPS, they contain NO INFO about Alice's identity, location or anything.



Now - while her phone sends out random messages, it also *listens* for messages from nearby phones.

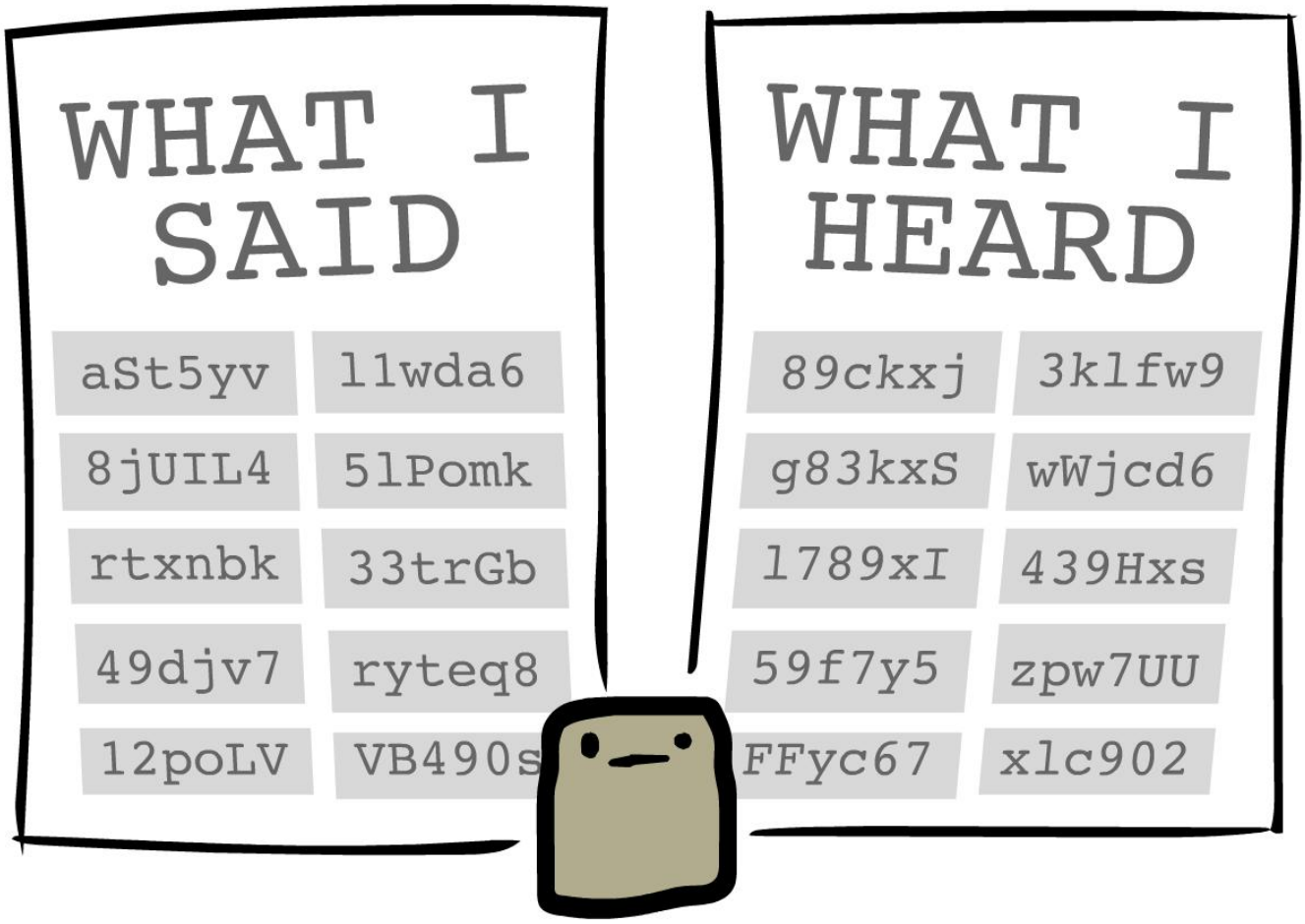
For example, Bob's.

Bob also has a privacy-first tracing app, that's compatible with (or the same as) Alice's.



If Alice & Bob stay close to each other for 5+ minutes, their phones will exchange unique gibberish.

Both their phones remember all the messages they said & heard over the last 14 days.



Again: because the random messages contain NO INFO, Alice's privacy is protected from Bob, and vice versa!

* 14 days is also just an example! epidemiologists may learn that the "infectious period" is actually shorter or longer.

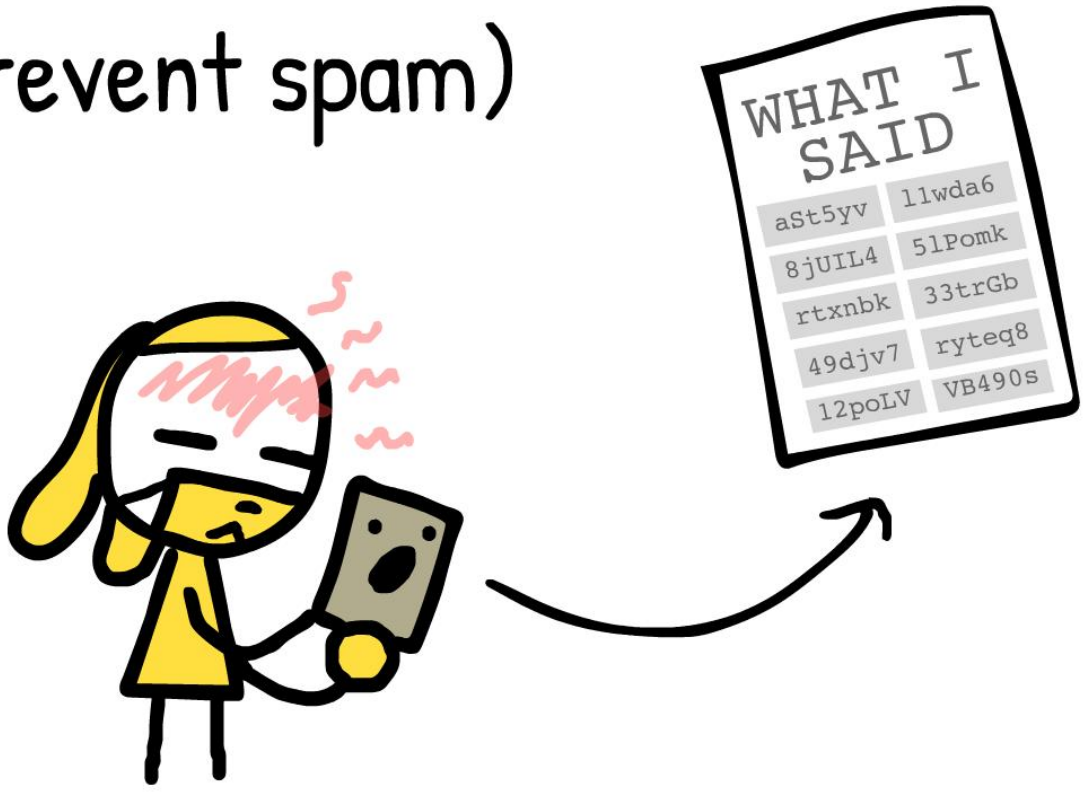
The next day, Alice develops a dry cough and fever.

Alice gets tested.

Alice has COVID-19.

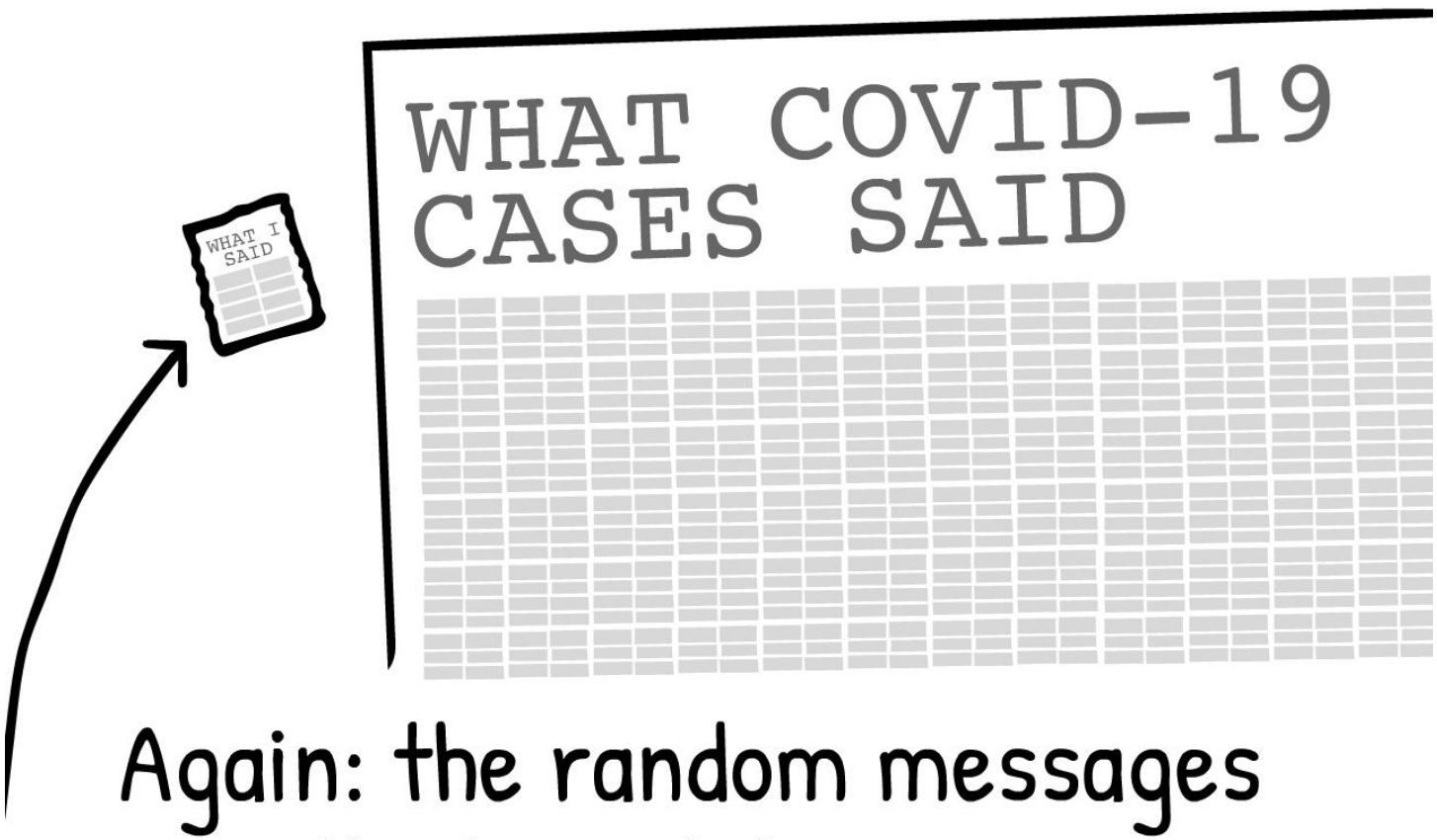
It is not a good day for Alice.

But she shan't suffer in vain! Alice uploads her "What I Said" messages to a hospital database, using a one-time passcode given by her doctor. (The code is to prevent spam)



Alice can also *hide* messages from times she wants to keep private, like evenings at home!

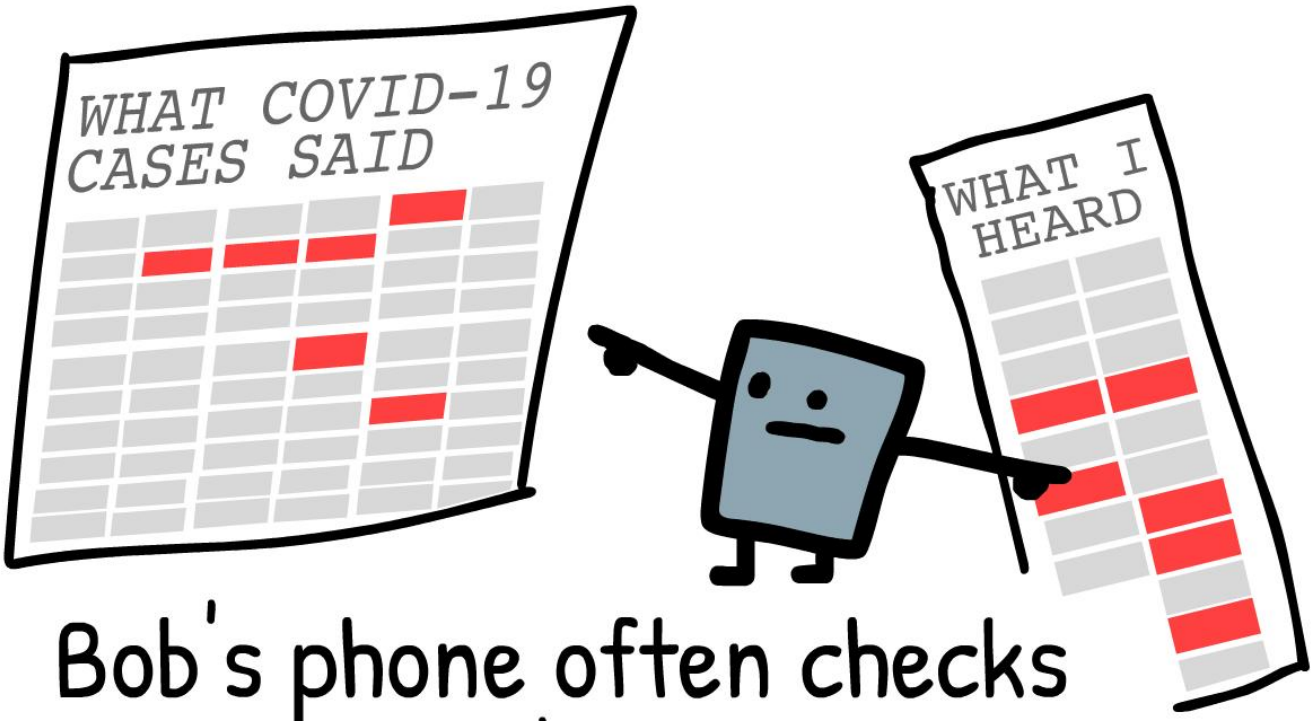
The database stores Alice's gibberish:



Again: the random messages give the hospital NO INFO on where Alice was, who she was with, what they were doing, or even *how many* people Alice met! It's meaningless to the hospital...

* different countries' hospitals could exchange messages, but because they contain no info, no privacy is lost.

...but not to Bob!

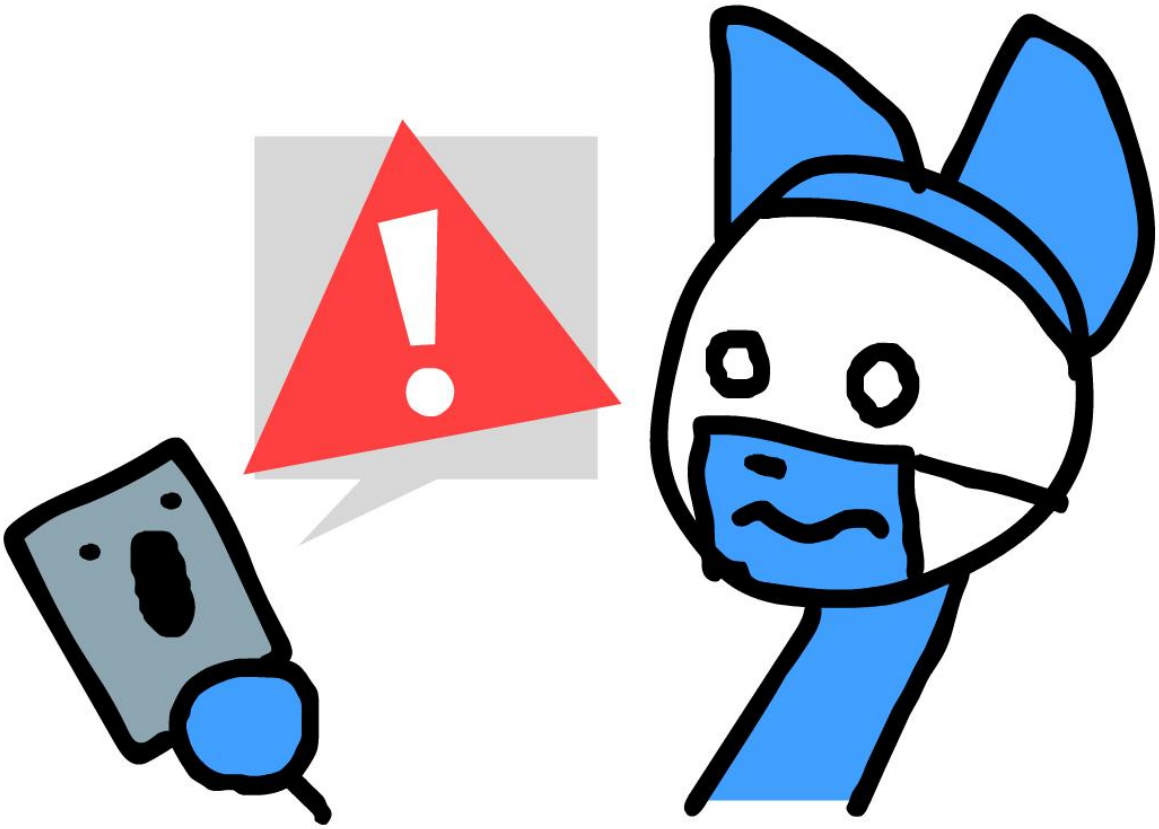


Bob's phone often checks the hospital's list of random messages from COVID-19 cases, and see if it "heard" any of them from nearby phones in the last 14 days.

(The gibberish gives Bob NO OTHER PERSONAL INFO.)

* the real DP-3T protocol is even MORE secure! it uses a "cuckoo filter" so phones know ONLY the covid-19 messages they heard, without revealing ALL covid-19 messages.

If it heard, say, 6 or more COVID-19 cases' messages (6 x 5 min = 30 min total exposure), the phone warns Bob to self-quarantine.

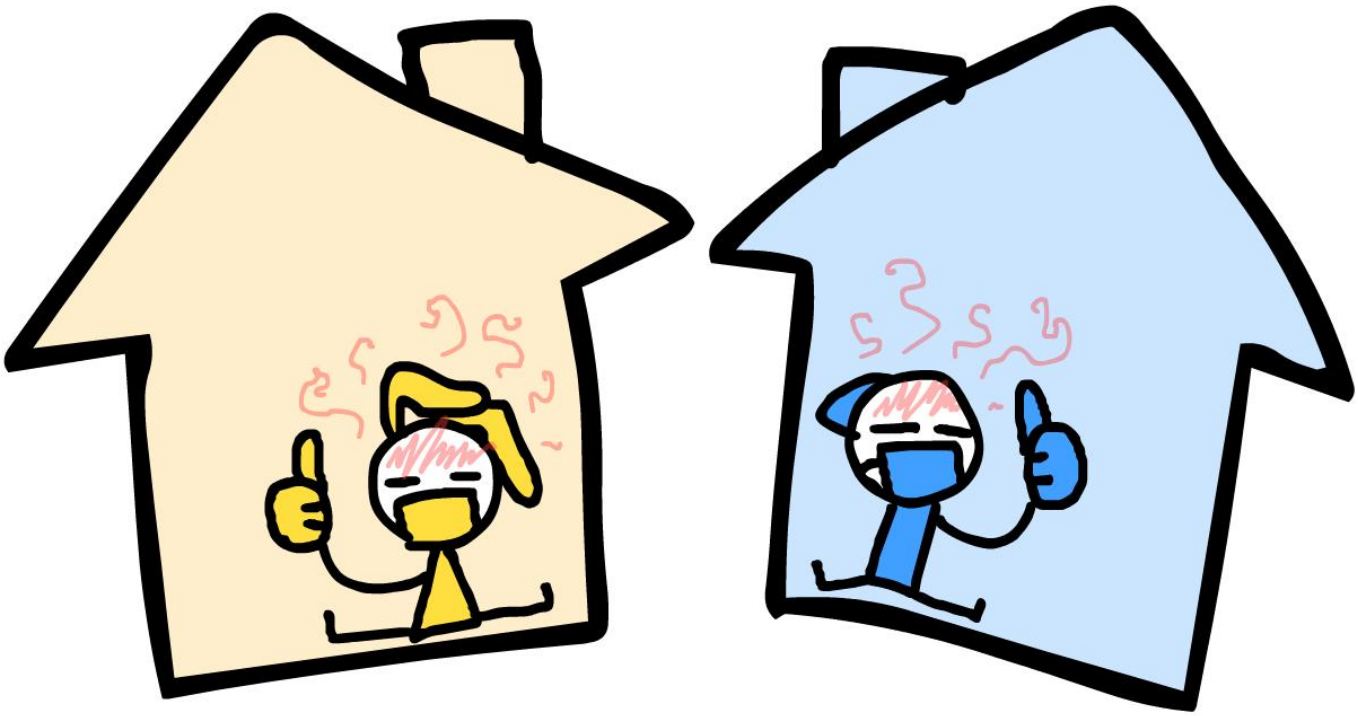


And thus, Bob cuts the chain of transmission - one step ahead of the virus!

* again, these numbers are just examples!

And that's it!

That's how digital contact tracing can proactively prevent the spread of COVID-19 *while also* protecting our rights.



Thanks, Alice & Bob!
Stay safe.

CITATIONS:

This comic is a rough summary of the **DP-3T** protocol, as of April 9th 2020. The real thing is more complex, and even *more* secure! See their paper:

github.com/DP-3T/documents

There's also another similar privacy-protecting system called **TCN Protocol.** Check that out here:

github.com/TCNCoalition/TCN

And finally, here's the University of Oxford study that showed contact tracing apps could contain COVID-19... *without* long-term lockdowns!

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

This comic is

PUBLIC DOMAIN

That means you *already* have permission to re-post this on your news site. Heck, we'd love it if you included it in your own contact tracing app! (as long as it *actually* follows the described privacy-protecting protocol)

(You also already have permission to translate this! The fonts used are "Patrick Hand" and "Open Sans")

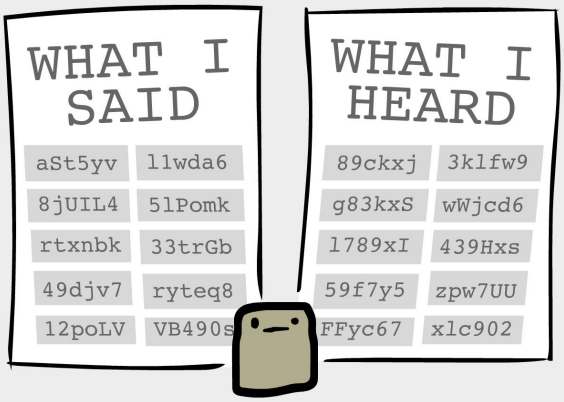
by **Nicky Case**
ncase.me + patreon.com/ncase

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

HOW PRIVACY-FIRST CONTACT TRACING WORKS

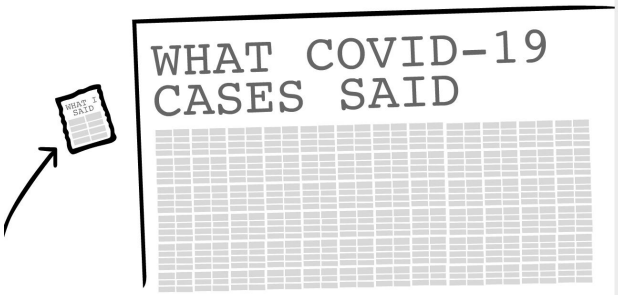
Alice's phone broadcasts a random message every few minutes.

Alice sits next to Bob. Their phones exchange messages.

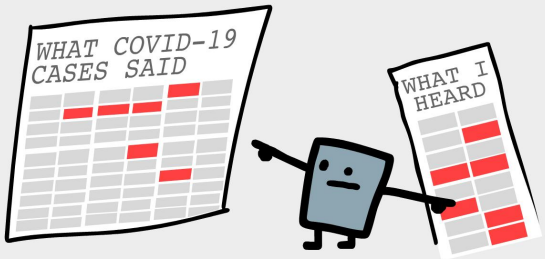


Both phones remember what they said & heard in the past 14 days.

If Alice gets Covid-19, she sends *her* messages to a hospital.



Because the messages are random, no info's revealed to the hospital...



...but Bob's phone can find out if it "heard" any messages from Covid-19 cases!

If it "heard" enough messages, meaning Bob was exposed for a long enough time, he'll be alerted.

And *that's* how contact tracing can protect our health *and* privacy!

by Nicky Case (ncase.me). CC0/public domain, feel free to re-post anywhere!