On Security, Privacy and Contact-Tracing

Prof. Janne Lindqvist

Department of Computer Science,

Aalto University

Director, Helsinki-Aalto Center for Information Security (HAIC)

June 16, 2020

CS-E4002: Human-Centred Research and Design in Crisis

Aalto University

Goals for this Lecture

Give basic tools for critical thinking about security and privacy designs

Related to contact tracing

And more generally

Spark interest in security (and privacy) engineering

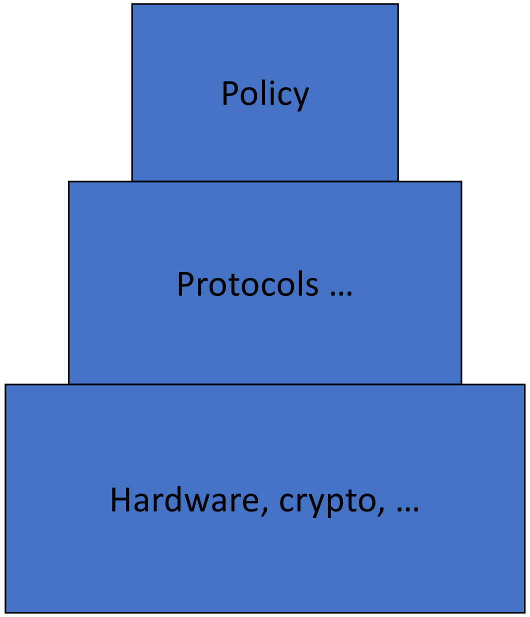
Aims in Security Engineering

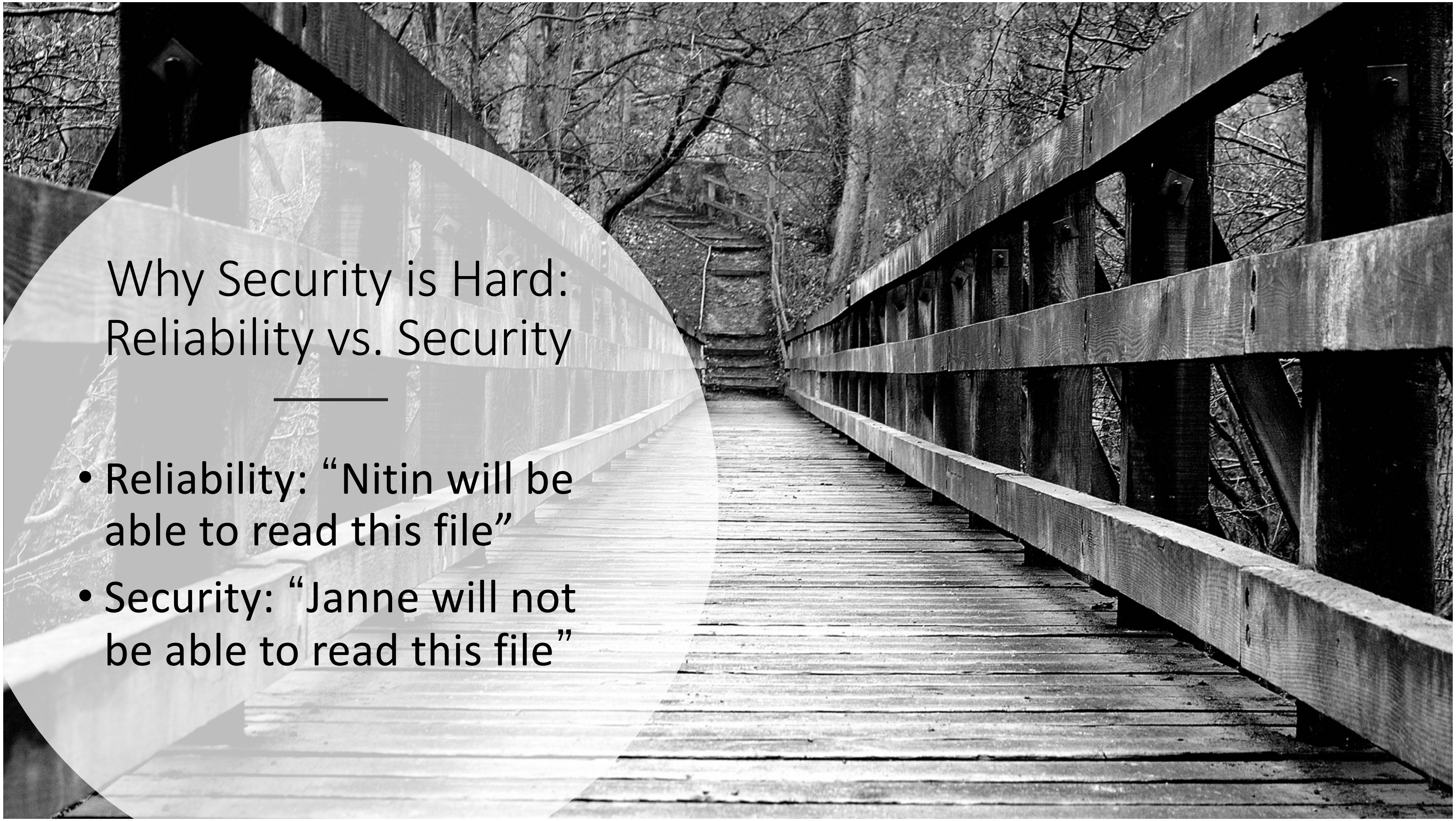
- High-level aims in Security Engineering
  - Policy
  - Mechanisms
  - Attacks
  - Assurance

- (For thorough understanding you need to take Aalto CS-E4350 Security Engineering, starting Spring 2021 ☺)

Security Engineering Design Hierarchy

- What are we trying to do?
- How?
- With what?





Why Security is Hard: Reliability vs. Security

- Reliability: “Nitin will be able to read this file”
- Security: “Janne will not be able to read this file”

Confusing(?) Terminology

- Secrecy
- Privacy
- Confidentiality
- Anonymity
- Pseudonymity
- Location Privacy
- Confidentiality (of communication)
- Confidentiality (of communication participants)
- Unlinkability

Classic Security: “CIA triad”

- Confidentiality
- Integrity
- Availability

- Has nothing to do with the other CIA – Central Intelligence Agency.

Threat Models?

- “Reports that say that something hasn't happened are always interesting to me, because as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns -- the ones we don't know we don't know. And if one looks throughout the history of our country and other free countries, it is the latter category that tend to be the difficult ones.”

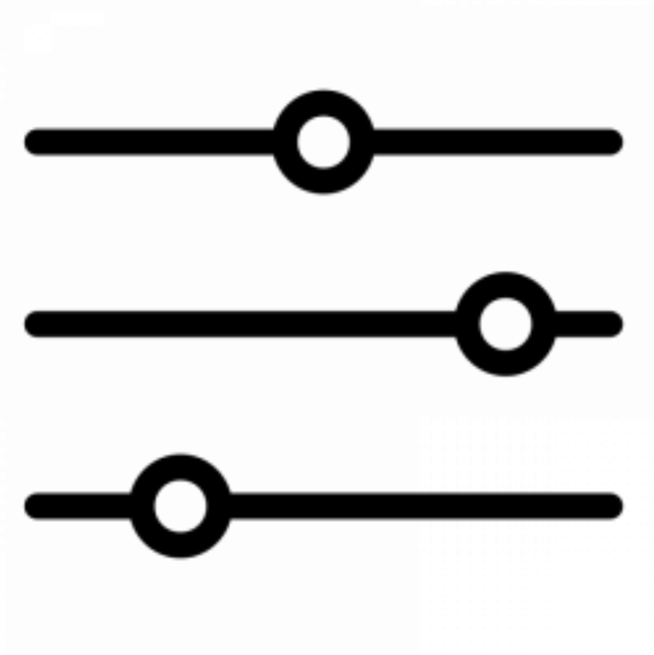
Threat Models?

- “Reports that say that something hasn't happened are always interesting to me, because as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns -- the ones we don't know we don't know. And if one looks throughout the history of our country and other free countries, it is the latter category that tend to be the difficult ones.” Donald Henry Rumsfeld, 21st Secretary of Defense from 2001 to 2006 under President George W. Bush.

Why Threat Models are Important?

Kanta

Design Space (not independent!)



Privacy-preserving — Privacy Invasive

Not Useful — Useful

Automated — Manual

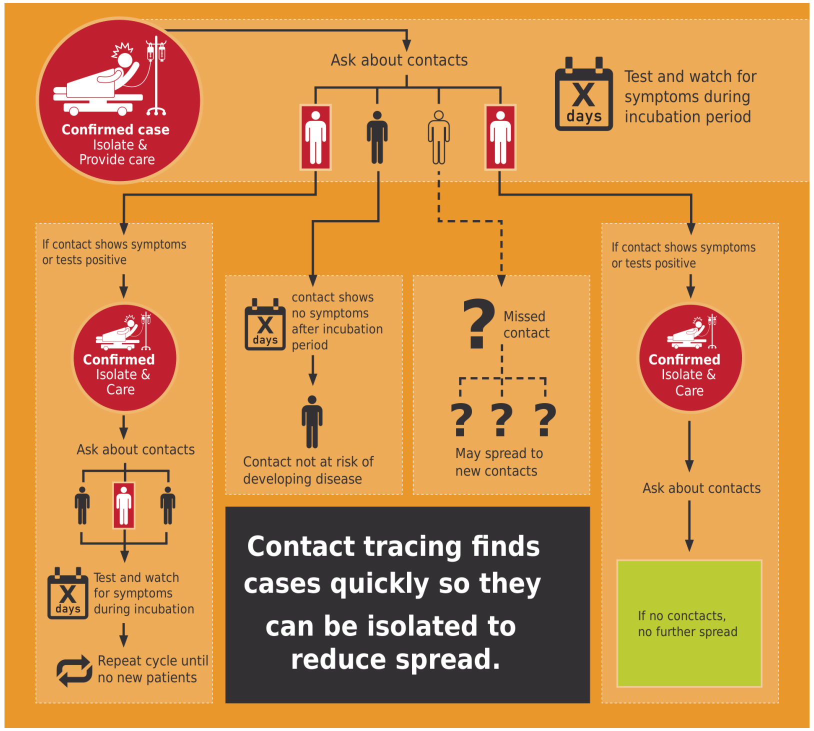
Design Space Scale

- Global scale (e.g. Apple/Google)
- Country scale ()
- Local scale (city?)
- Ultralocal (one company, hospital, university, school?)

GOALS????

Ought [to] this be done?

What is Contact Tracing?



Confirmed case
Isolate &
Provide care

Ask about contacts

X days Test and watch for symptoms during incubation period

If contact shows symptoms or tests positive

Confirmed
Isolate &
Care

Ask about contacts

X days Test and watch for symptoms during incubation

Repeat cycle until no new patients

X days contact shows no symptoms after incubation period

Contact not at risk of developing disease

Missed contact

? ? ?

May spread to new contacts

If contact shows symptoms or tests positive

Confirmed
Isolate &
Care

Ask about contacts

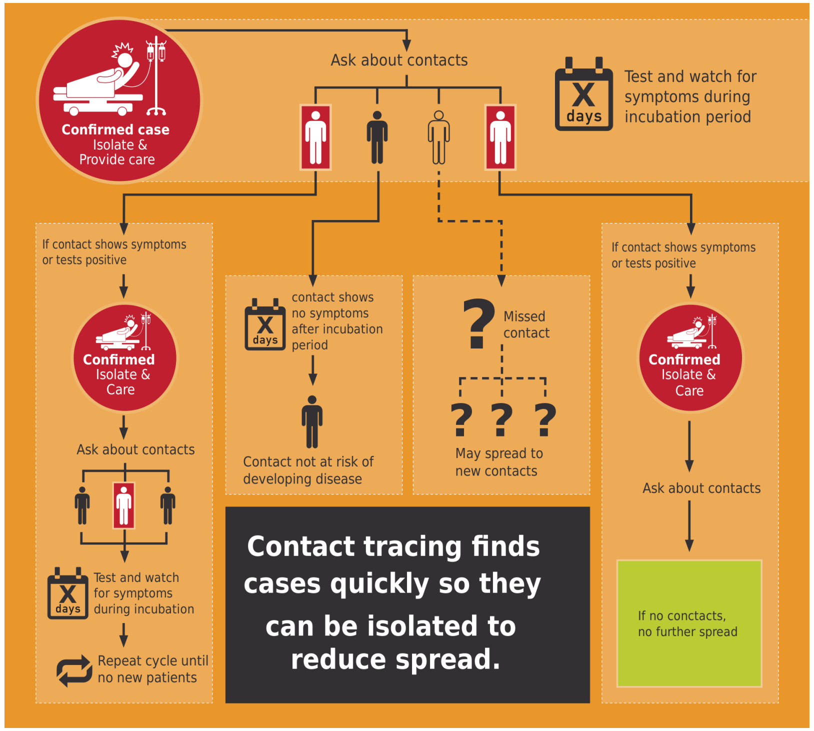
If no conctacts, no further spread

Contact tracing finds cases quickly so they can be isolated to reduce spread.

CDC, Wikipedia, CC BY-SA 4.0

- “To interrupt ongoing transmission and reduce the spread of an infection
- To alert contacts to the possibility of infection and offer preventive counseling or prophylactic care
- To offer diagnosis, counseling and treatment to already infected individuals
- If the infection is treatable, to help prevent reinfection of the originally infected patient
- To learn about the epidemiology of a disease in a particular population”

What is Contact Tracing?

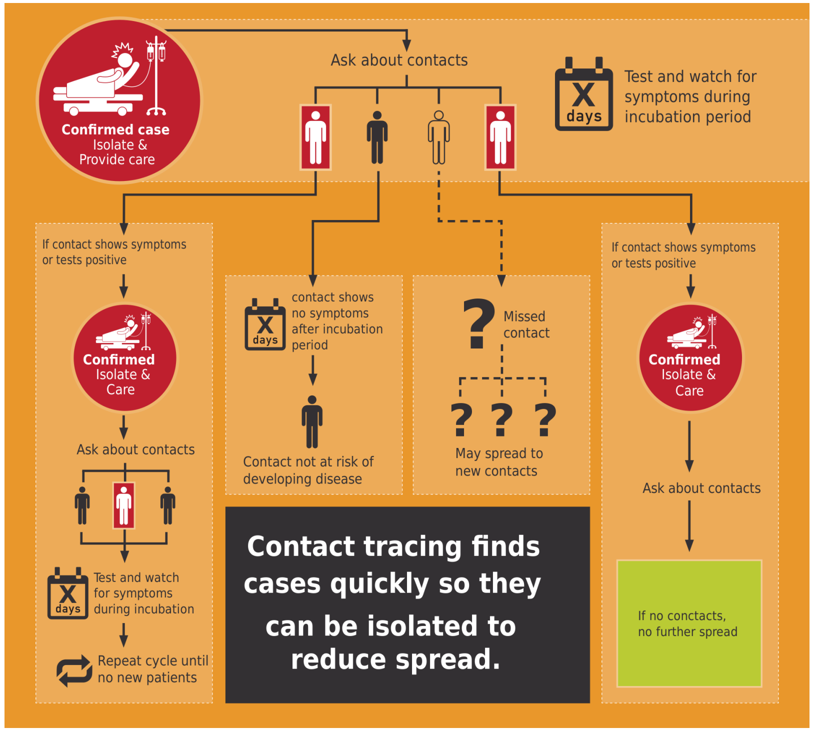

Confirmed case
Isolate &
Provide care
Ask about contacts
X
days
Test and watch for symptoms during incubation period
If contact shows symptoms or tests positive
Confirmed
Isolate &
Care
Ask about contacts
X
days
Test and watch for symptoms during incubation
Repeat cycle until no new patients
X
days
contact shows no symptoms after incubation period
Contact not at risk of developing disease
?
Missed contact
? ? ?
May spread to new contacts
If contact shows symptoms or tests positive
Confirmed
Isolate &
Care
Ask about contacts
If no conctacts, no further spread

Contact tracing finds cases quickly so they can be isolated to reduce spread.

CDC, Wikipedia, CC BY-SA 4.0

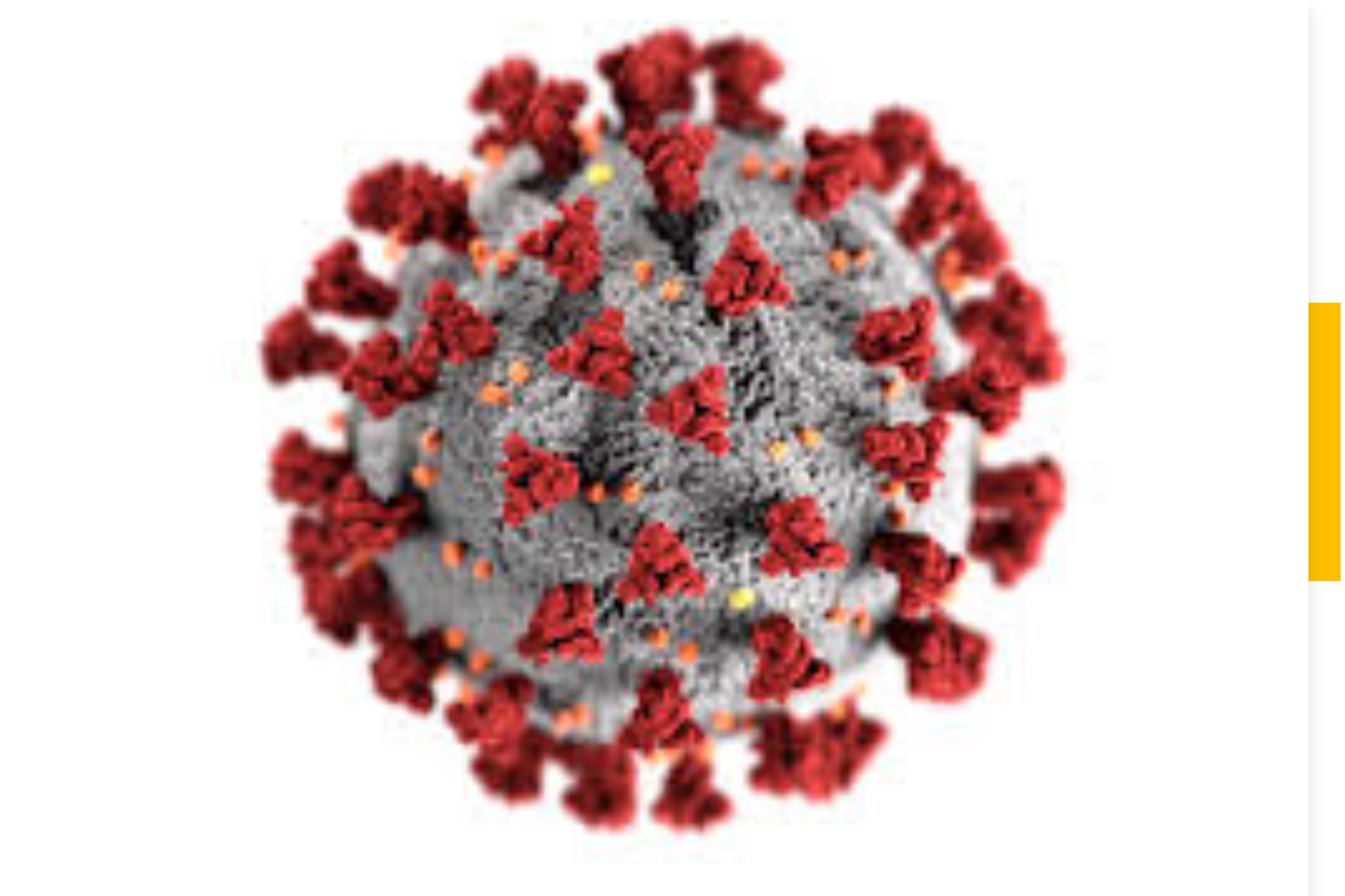
- Manual contact tracing is hard work done by professionals.
- What about privacy?

What is Contact Tracing?


Confirmed case
Isolate &
Provide care
Ask about contacts
X days
Test and watch for symptoms during incubation period
If contact shows symptoms or tests positive
Confirmed
Isolate &
Care
Ask about contacts
X days
Test and watch for symptoms during incubation
Repeat cycle until no new patients
X days
contact shows no symptoms after incubation period
Contact not at risk of developing disease
?
Missed contact
? ? ?
May spread to new contacts
If contact shows symptoms or tests positive
Confirmed
Isolate &
Care
Ask about contacts
If no conctacts, no further spread
Contact tracing finds cases quickly so they can be isolated to reduce spread.

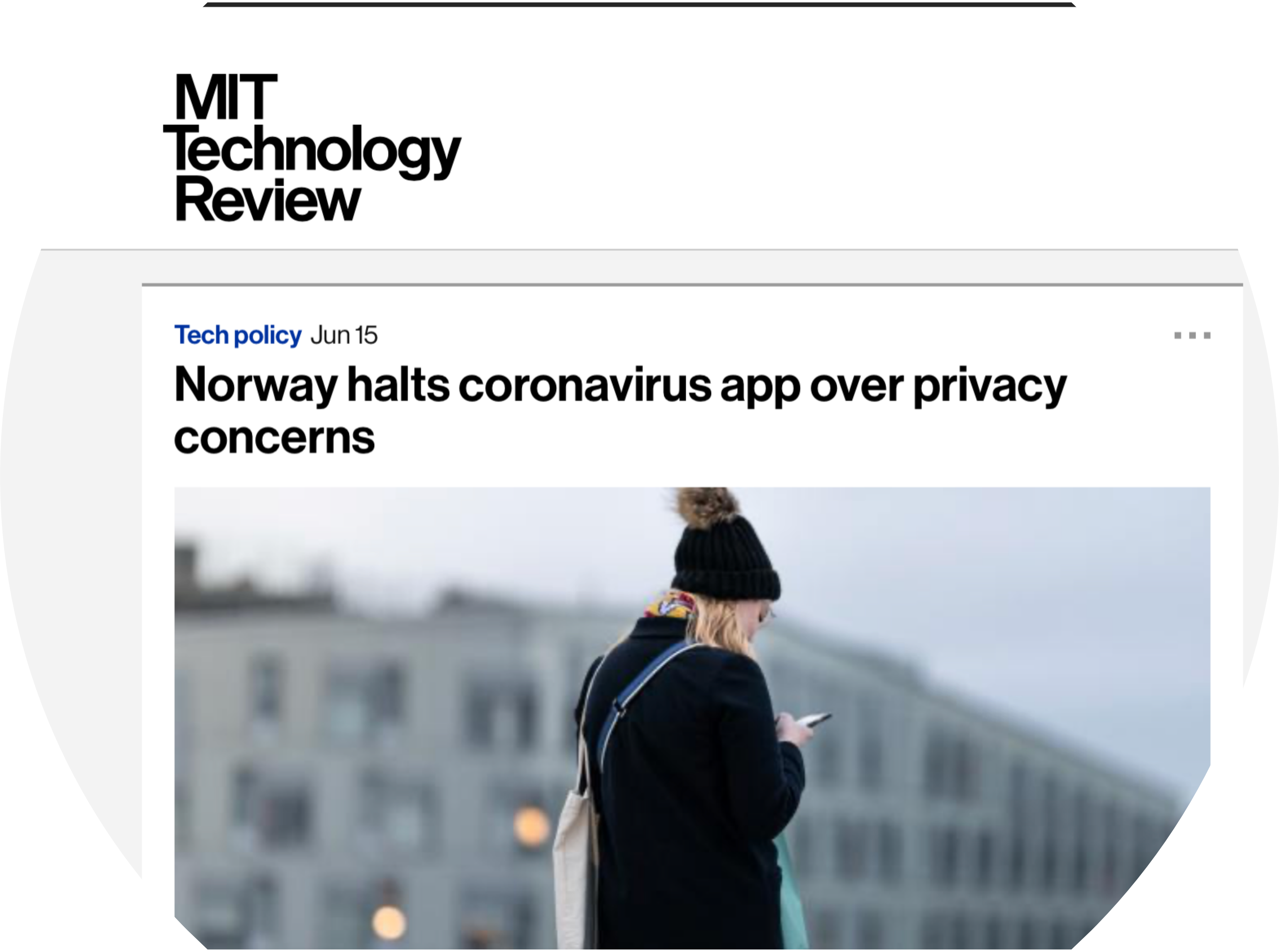
CDC, Wikipedia, CC BY-SA 4.0

- Secrecy
- Privacy
- Confidentiality
- Anonymity
- Pseudonymity
- Location Privacy
- Confidentiality (of communication)
- Confidentiality (of communication participants)
- Unlinkability



Enter COVID-19

“There’s an app for that!”



MIT Technology Review

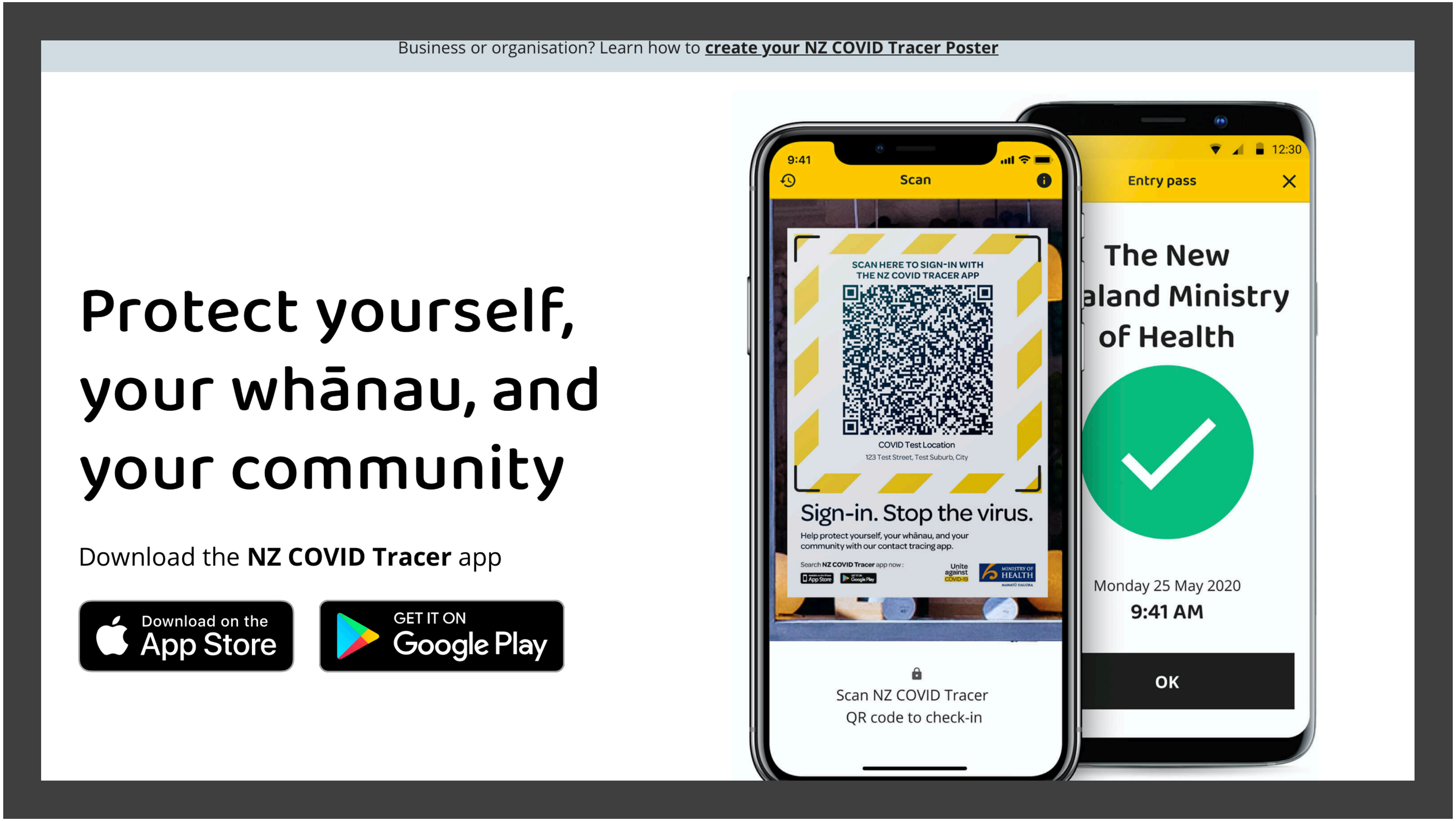
Tech policy Jun 15

Norway halts coronavirus app over privacy concerns

Confusing(?) Terminology

- Secrecy
- Privacy
- Confidentiality
- Anonymity
- Pseudonymity
- Location Privacy
- Confidentiality (of communication)
- Confidentiality (of communication participants)
- Unlinkability

Ought [to] this have been done?



Business or organisation? Learn how to **create your NZ COVID Tracer Poster**

Protect yourself, your whānau, and your community

Download the **NZ COVID Tracer** app

Download on the App Store
GET IT ON Google Play
9:41
Scan
SCAN HERE TO SIGN-IN WITH THE NZ COVID TRACER APP
COVID Test Location
123 Test Street, Test Suburb, City
Sign-in. Stop the virus.
Help protect yourself, your whānau, and your community with our contact tracing app.
Search NZ COVID Tracer app now :
Unite against COVID-19
MINISTRY OF HEALTH
Scan NZ COVID Tracer QR code to check-in
12:30
Entry pass
The New aland Ministry of Health
Monday 25 May 2020
9:41 AM
OK

Confusing(?) Terminology

- Secrecy
- Privacy
- Confidentiality
- Anonymity
- Pseudonymity
- Location Privacy
- Confidentiality (of communication)
- Confidentiality (of communication participants)
- Unlinkability

Ought [to] this have been done?

SKETCH

Design Space Scale

- Global scale (e.g. Apple/Google)
- Country scale ()
- Local scale (city?)
- Ultralocal (one company, hospital, university, school?)

Contact Tracing?

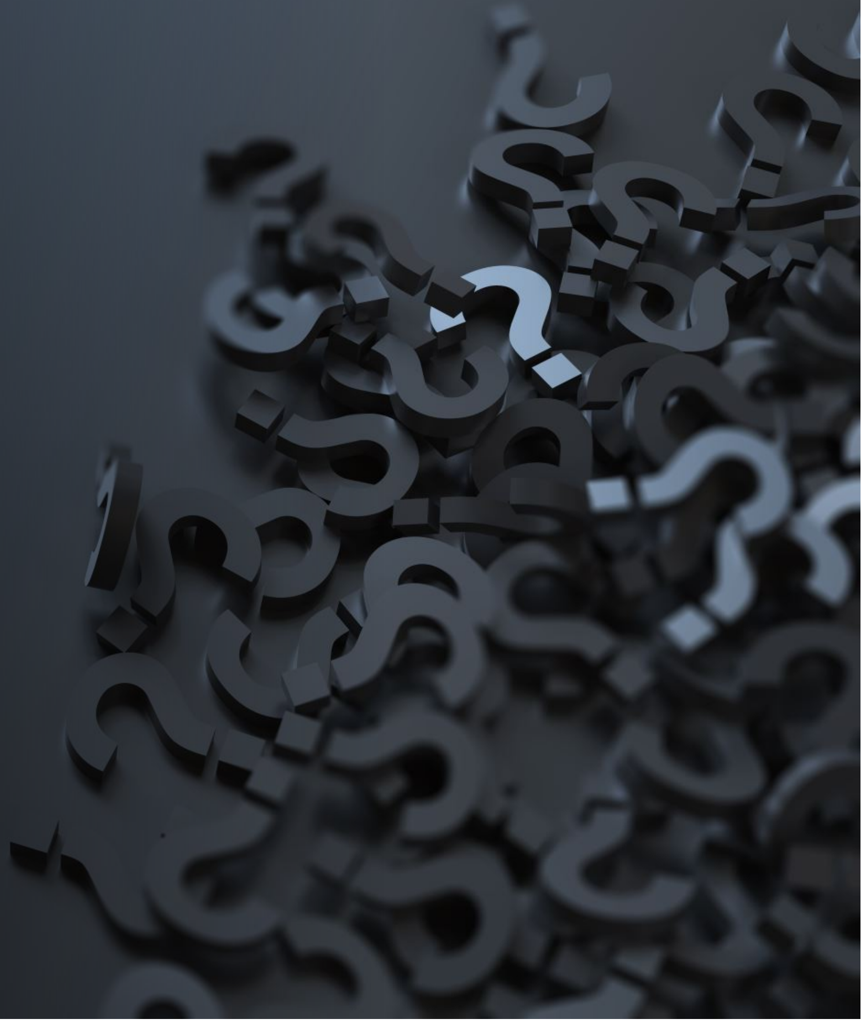
Ought [to] this be done?

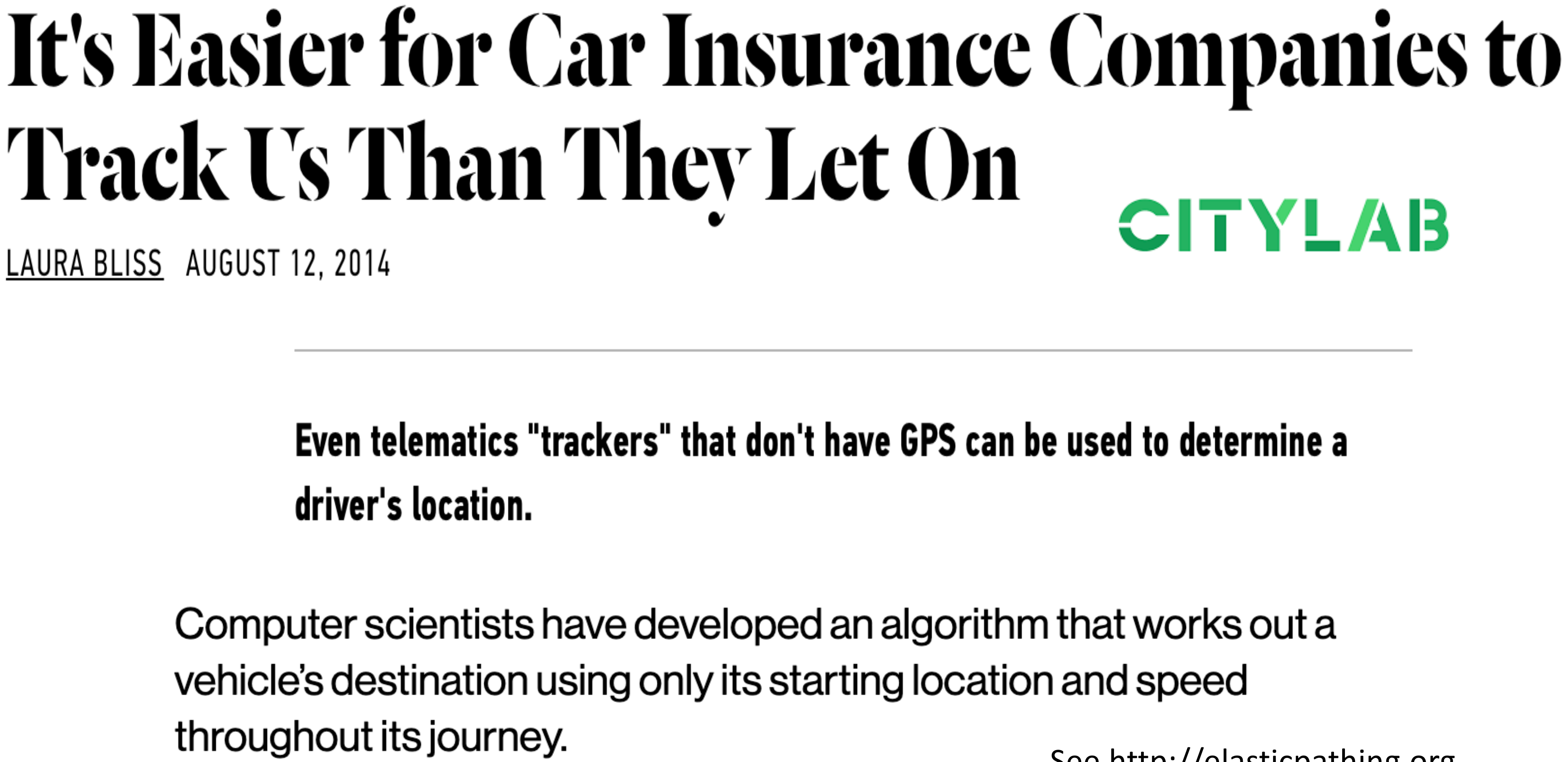
Targeted identifiable tracing at ultra-local scale

- For example, in the US you must have a wrist-band to visit hospitals.

- How about a broadcast wrist-band that broadcasts an identifier?
- Hospital staff, patients and visitors must wear when entering the premises.

FINAL REMARKS





It's Easier for Car Insurance Companies to Track Us Than They Let On

CITYLAB

LAURA BLISS AUGUST 12, 2014

Even telematics "trackers" that don't have GPS can be used to determine a driver's location.

Computer scientists have developed an algorithm that works out a vehicle's destination using only its starting location and speed throughout its journey.

See http://elasticpathing.org

Security Engineering

- It is about trade-offs
- If somebody says something is “totally” secure and privacy-preserving, chances are
    - They don’t know what they are talking about
    - They are lying
    - They have something to gain
    - All of the above

Thank You!

JANNE.LINDQVIST@AALTO.FI

LINDQVISTLAB.ORG (TO BE UPDATED SOME DAY!)

HAIC.FI

Next Tuesday:

Designing for Healthcare Experiences from a Multi-stakeholder Perspective

Prof. Johanna Kaipio, Department of Computer Science, Aalto University

Aalto University
School of Science