Perspectives on Digital Contact Tracing

Ronald L. Rivest
MIT Institute Professor

Algorithm Design, Law, and Policy Workshop
Simons Institute, Berkeley
July 20, 2020
Outline

• (Disambiguation Page)
• Manual Contact Tracing
• Digital Contact Tracing
• Ranging Accuracy – TC4TL (Too Close For Too Long)
• Privacy
• Integration with PH
• Adoption
• Effectiveness
• Law
• Policy
• Conclusions
(Disambiguation Page)

• PACT (aka “PACT-East”) *
  “Private Automated Contact Tracing”
  http://pact.mit.edu/

• PACT (aka “PACT-West”) 
  “Privacy Sensitive Protocols and Mechanisms for Mobile Contact Tracing”
Manual Contact Tracing (MCT)

• When a person (“index case”) tests positive, finding all or most of the people he may have exposed (“contacts”) is called contact tracing.

• Manual CT is based on interviews with the index case, and phone calls to contacts.

• CT allows contacts to be quarantined, symptom-checked, and tested.

• CT is a powerful method for “flattening the curve”, as it removes infectious people from circulation.

• Classic method, used widely for many pandemics.

• Limitations: speed, compliance, and recall ability.
Digital Contact Tracing

• PACT protocol inspired by Apple “Find My” (taught by Yael Kalai and me in Spring 2020 security course)
• Uses Bluetooth by Apple devices to sense proximity.
• Phone broadcasts values; these change frequently for privacy protection.
• Public DB allows owner to find “where lost phone was last seen” while protecting privacy.
• PACT protocol is similar: phone broadcast changing “chirps”.
• If owner tests positive, can upload to DB the seeds for generating chirps.
• Others can check parties in a decentralized manner if they have heard chirps of infected.
• Similar protocols developed concurrently: DP3T, TCN, ...
• Dozens of countries now rolling out such apps...
PACT (East) team

• PACT organized early March
• Leadership:
  • MIT campus: me, Danny Weitzner
  • MIT Lincoln Lab: Marc Zissman, Israel Soibelman
  • MGH: Louise Ivers (Medical / Public-Health advisor)
• Many organizations represented: MIT, MIT Lincoln Lab, MGH, Weizmann, BU, Brown, IBM, CMU, MITRE, Northeastern, Qualcomm, Sandia, ...
• > 100 people (particularly strong on “layer 1” = BT ranging)
• Strong relationships with other teams, Apple|Google, other vendors, jurisdictions, public health, ...
• PACT role: technology evaluator and advisor, not app developer; more interest in “helping good things happen” than “taking credit”
TC4TL Accuracy (Distance & Time)

• CDC says “too close for too long” should be < 6 feet for > 15 minutes.
• BT is for local communications (<30m) -- can it be used for ranging?
• Received signal strength (RSSI) depends on:
  • Transmitter power
  • Phone orientation (carriage)
  • In-pocket / out-of-pocket
  • Indoors / Outdoors (multipath)
  • Intervening bags of water (bodies!) – but not intervening walls!
• This may be the biggest challenge for BT-based contact tracing.
TC4TL (Cont.)

• Getting sufficient samples can also be dicey (battery drain!)

• MIT LL has put incredible effort into BT phenomenology

• Data Collection Coalition – collects BT ranging data

• NIST challenge applying ML to TC4TL: https://www.nist.gov/itl/iad/mig/nist-tc4tl-challenge

• PACT also exploring fixed beacons, wearables, ultrasound, UWB
Privacy

• No data leaves phone without user consent.
• No usage of GPS location.
• Phone broadcasts changing pseudorandom “chirps”, so no tracking.
• Phone records “chirps it has heard”
• Infected users (who test positive) may post seeds for their chirps.
• Phone matches (locally!) against posted DB of “infected chirp seeds”
  • No need for central DB to store sensitive personal information
• Match causes user to be alerted (stay-at-home, watch symptoms, test!)
• Extensions exist for dealing with replay & relay attacks.
Integration with Public Health

• Goal is to *improve* and *extend* manual contact tracing, not to *replace* it.

• Contacts need information about what to do, where to obtain support services, etc.

• Digital contact tracing should feed into MCT software.

• Digital contact tracing can make MCT *faster* and *more complete*.
Adoption can be a challenge

• For DCT to be effective, *both* parties need to be running DCT service.

• So 50% adoption rate may mean only 25% of contacts get logged.

• Apple and Google have announced **AEN (Automatic Exposure Notification)**, an API in iPhones **and** Androids, providing **interoperability**. *(A huge, and very welcome, development! Thanks, A|G!!)*

• People may resist adoption because:
  • Fear of “big brother” (privacy concerns; police; ICE; housing)
  • Confusing UI (e.g. request on Android for “location services” permission)

• Rollouts in EU (Switzerland, Germany, Denmark) have >10% so far.
Effectiveness

• Can digital contact tracing really help? Can it save lives?

• Ferretti et al. (*Science, May 8 2020*) show via model:
  “Immediate notification through a contact-tracing mobile phone app could, however, be sufficient to stop the epidemic if used by a sufficiently high proportion of the population.”

• Singapore: digital contact tracing does reveal new contacts, beyond those found by manual contact tracing.

• DCT may allow for *faster* alerts of duplicate contacts.

• But: *mask-wearing* may decrease number of *strangers* you infect, and thus decrease utility of DCT...
Venn Diagram

- Numbers are made-up (100 total).
- **New** contact (1 in pink) discovered by DCT.
- **Duplicate** contacts (17 in green) can get faster notification.
Law

Most interesting legal questions (?):

- Can law enforcement access or use contact-tracing information in any way?
- Do we need to update laws concerning protection and sharing of medical data, for handling DCT data?
Policy

- Can/should app use be made mandatory? (e.g. for jurisdictions, services, businesses, schools??)
- Tension between Public Health and Privacy: more information revealed to system may improve public health results, at a cost to privacy:
  - GPS data
  - “who infected me?”
- Who decides policy: government or high-tech?
- How/whether to turn off DCT when this pandemic is over?
Conclusions

• We have come a long ways since COVID-19 appeared, including:
  • Decentralized privacy-preserving protocols
  • Much better understanding of BT phenomenology
  • Apple-Google collaboration on AEN API

• Yet there remain significant challenges:
  • Improving ranging accuracy
  • Dealing with fragmented nature of US health care
  • Achieving sufficient adoption rates