Privacy at the time of Pandemic

Stan[isław] Matwin

IPI PAN
Institute for Big Data Analytics

Dalhousie University, Halifax, Kanada

- What is this talk about
- Some epidemiological facts
  - 3 ways of bounding R0
- Testing, tracking and tracing
- The main track-and-trace approaches and apps
- Privacy challenges
- Policy challenges

3 ways of bounding R0

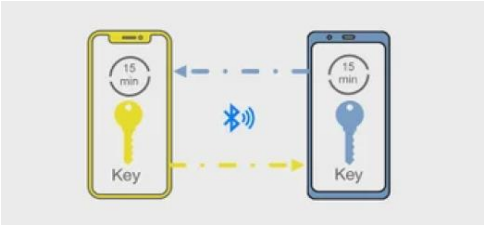
- Vaccine
- Herd immunity
- Test, track and trace

Test, track and trace

- Key for exiting from confinement
- The very idea
  - Testing as many people as possible
  - For the positives, identifying **iteratively** their contacts
- The broader the testing, the better (100%!)
- Tracing cannot be done manually at scale
- Mobile phone as a tracing device
  - South Korean example

Mobile phone info for Track-and-trace

- Proximity – BlueTooth (contact distance, duration are parameters)



- Spatial information (clusters, super-spreaders,…)

Track and trace apps

- Tracktogether – Singapore
- Google-Apple proposal
- European proposal

Terminology:
BT= Bluetooth

Positive= infected person

HA= Health authority (gov't)

TrackTogether

- Singapore, implemented and used at scale since Mar. 20 [Choo et al.2020]
- Proximity tracing via BT: nearby phones exchange tokens, also sent to HA
- Positives release their contacts to the HA (legal obligation)
- HA has the mapping of tokens to ID, **CAN TAKE ACTION**
  - notify Positive's contacts
  - Isolate the Positive (provably via phone tracing)
- Tokens have limited lifespan (in minutes)
- Opting in?
- Participation rate?

Google-Apple [Wired 20]

- Proposed design
- Proximity tracing via BT
- Tokens: user A's phone stores $P_A(14)$ = anonymous tokens of all A's contacts (14 days)
- *A*'s contact *B* tests Positive
- *B* uploads all their tokens to a server (HA?)
- User *A* check server periodically, downloads all positives *P(14)*
- Since $B \in P_A(14)$, *A* is notified, told about further action
- No HA actionability, but can be added
- Baked into the OS
  - battery life
  - interoperability
- Opt-in

Potential actionablility

- *A* tests
- Test result is entered into the app
  - If negative, no action
  - If positive, *A* needs to at least self-isolate, which can be enforced by the app easily and privately.
  - A violation of the self-isolation would be reported by the app to HA

European idea ([Nanni et al. 201: 40/14

TRANSACTIONS ON DATA PRIVACY 13 (2020) 61–66

- Privacy-safe, spatially-oblivious proximity tracing: BT **+ spatio-temporal:**
  - [DP3T] (Decentralized Privacy-preserving Proximity Tracing) model
- Opt-in
- Based on Personal Data Store framework: user control release
  - What
  - To whom
  - Trust!
- Potentially privacy sensitive
- Insistence on
  - Use Limitation Principle
  - Data auto-destruction

Give more data, awareness and control to individual citizens, and they will help COVID-19 containment

Mirco Nanni[1,*], Gennady Andrienko[2,3], Albert-László Barabási[4], Chiara Boldrini[5], Francesco Bonchi[6,7], Ciro Cattuto[8,6], Francesca Chiaromonte[9,10], Giovanni Comandé[9], Marco Conti[5], Mark Coté[11], Frank Dignum[12], Virginia Dignum[12], Josep Domingo-Ferrer[13], Paolo Ferragina[14], Fosca Giannotti[1], Riccardo Guidotti[14], Dirk Helbing[15], Kimmo Kaski[16], Janos Kertesz[17], Sune Lehmann[18], Bruno Lepri[19], Paul Lukowicz[20], Stan Matwin[21,22], David Megías Jiménez[23], Anna Monreale[14], Katharina Morik[24], Nuria Oliver[25,26], Andrea Passarella[5], Andrea Passerini[27], Dino Pedreschi[14], Alex Pentland[28], Fabio Pianesi[29], Francesca Pratesi[14], Salvatore Rinzivillo[1], Salvatore Ruggieri[14], Arno Siebes[30], Vicenç Torra[31,32], Roberto Trasarti[1], Jeroen van den Hoven[33], Alessandro Vespignani[4]

* E-mail: mirco.nanni@isti.cnr.it

[1] ISTI-CNR, Italy; [2] IAIS-Fraunhofer, Germany; [3] City University of London, UK; [4] Northeastern University, USA; [5] IIT-CNR, Italy; [6] ISI Foundation, Italy; [7] Eurecat, Spain; [8] University of Torino, Italy; [9] Sant'Anna School of Advanced Studies Pisa, Italy; [10] Penn State University, USA; [11] King's College London, UK; [12] Umeå University, Sweden; [13] Universitat Rovira i Virgili, Catalonia; [14] University of Pisa, Italy; [15] ETH Zurich, Switzerland; [16] Aalto University School of Science, Finland; [17] Central European University, Hungary; [18] Technical University of Denmark; [19] FBK, Italy; [20] DFKI, Germany; [21] Dalhousie University, Canada; [22] Polish Academy of Sciences, Poland; [23] Universitat Oberta de Catalunya; [24] TU Dortmund University, Germany; [25] ELLIS Alicante, Spain; [26] Data-Pop Alliance, USA; [27] Università degli Studi di Trento; [28] MIT, USA; [29] EIT Digital, Italy; [30] Universiteit Utrecht, The Netherlands; [31] Maynooth University, Ireland; [32] Skövde University, Sweden; [33] TU Delft, The Netherlands

Abstract. The rapid dynamics of COVID-19 calls for quick and effective tracking of virus transmission chains and early detection of outbreaks, especially in the "phase 2" of the pandemic, when lockdown and other restriction measures are progressively withdrawn, in order to avoid or minimize contagion resurgence. For this purpose, contact-tracing apps are being proposed for large scale adoption by many countries. A centralized approach, where data sensed by the app are all sent to a nation-wide server, raises concerns about citizens' privacy and needlessly strong digital surveillance, thus alerting us to the need to minimize personal data collection and avoiding location tracking. We advocate the conceptual advantage of a decentralized approach, where both contact and location data

Privacy dimensions [Choo 20]

- Inadequacy of existing data privacy frameworks, eg Differential Privacy
- Need for a new approach
- [Choo et al 20] propose:
  - Privacy from hackers:
    - Thought experiment – data sent in the open: even anonymizing the user with a unique ID **IS INADEQUATE**: linking attack (eg via social networks, spatio-temp info)
    - sending random, time-varying tokens instead
  - Privacy from contacts: TT does not reveal Positive's info
  - Privacy from HA

Apps - comparison

	TraceTogether	Googe/Apple	EU PDS
opt in/opt out	Y	Y[1]	Y
distributed	N	Y	Y
actionable	Y	N	N
privacy contacts	Y	Y	?
Privacy HA	N	Y[1, 2]	Y[3]
Spatio-temporal	N	N	Y

1) what when it's embedded in the OS?

2) unclear whether has access to the IP address of the user?

3) the user may give HA access.

Discussion

- Requirements for T&T to work epidemiologically
  - ACTIONABILITY
  - Coverage – 60%?
  - People without smartphones (Canada – 16%; Poland 30%)
- Policy challenges
  - Volunteer or compulsory (opt in-out)

Other crucial requirements

- Data autodestruction
- Sunset clause
- Use Limitation Principle

Data autodestruction

- Clearly normal OS “delete” functions inadequate
- Cryptograhic techniques exist that will effectively make data inaccessible on a trigger (could be date)
  - Data is encrypted and key is deleted on trigger
- Computationally heavy
- Can we guarantee key deletion?
- New solutions are needed
  - eg memories erasable by physical process – eg power off?

Sunset clause

Guarantee that the data collection will stop at a given time

- Defining that time
  - epidemiologically?
  - Periodically?

Guaranteeing that data is NOT collected

- Code inspection – by whom?
- Automatic code verification?

ULP guarantee

- Use Limitation Principle [OECD 2013]:
  - purpose form which the data is collected is declared upfront
  - data is ONLY used for the purpose
- How can we guarantee how the data is used?
- App code
  - Code inspection
  - Code property verification using program proving tools/techniques (e.g. [Matwin, Felty 03]
  - Computationally not scalable at present

Other tech T&T and similar proposals

- Quarantine enforcement
- Temperature monitoring
- Mask use and separation monitoring

Policy challenges

- Putting trace-and-track systems/apps in place – by whom?
  - Parliamentary decision, time limited
- Monitoring compliance with privacy requirements
  - A trusted, mixed body: gov't, industry, academia (modeled on security…)

References

- [Choo et al 20], Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs, 2020
- [DP3T 20] (Decentralized Privacy-pteserving Proximity Tracing, https://github.com/DP-3T/documents
- [Nanni et al. 20] Give more data, awareness and control to individual citizens, and they will help COVID-19 containment, Trans. On Data Privacy, 13(2020), 61-66
- [Felty, Matwin 02] Amy Felty, Stan Matwin: Privacy-Oriented Data Mining by Proof Checking. PKDD 2002: 138-149
- [Matwin 20a] Matwin, S. Privacy at the times of Pandemic: https://bigdata.cs.dal.ca/sites/default/files/Privacy_at_the_time_of_pandemic_15_04_20_SM_clean.pdf
- [Matwin 20b] https://www.project-syndicate.org/commentary/covid19-lockdowns-end-with-track-and-trace-by-stan-matwin-2020-04?fbclid=IwAR0azd61WHQGtTJUPRVJ7FabROevJ2nPSIz9MRdD15PfL7mCJaR_zT_lpoQ
- [Matwin 20b WERSJA POLSKA]: https://wyborcza.pl/magazyn/7,124059,25908313,prof-stan-matwin-wszystkich-nie-przetestujemy-trzeba.html
- [OECD 13] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm
- [Wired 20] How Apple and Google Are Enabling Covid-19 Contact-Tracing, Wired, 10/4/20

Nie czas żałować róż, gdy płoną lasy

Juliusz Słowacki
1809-1849

Właśnie gdy płoną lasy, należy ratować róże

Janusz Korczak
1879-1942