CONTACT TRACKING APPS 'EXPOSURE NOTIFICATION' API

Mireille Hildebrandt

- issues
- distinctions
- law, code & ethics
- jurisdiction: law and rule of law
- [Tracetogether, PEPP-PT, DP-3T, NHSX] API GAPPLE
- references

issues

1. Do we need a contact tracking APP?
   - tool for crowd control (due to the alerts)
   - potential infringement of a number of fundamental rights (privacy, non-discrimination, due process, freedom of speech, freedom of association, freedom of movement)

- If infringement: legal basis, legitimate aim, NECESSITY, proportionality
- If not effective it cannot be necessary or proportional

issues

2. Do we need a contact tracking APP?
   - Advantages re manual tracking (limits human memory, unknown contacts)
     - Contacts during incubation period
   - Disadvantages re manual tracking (sterile alerts, confusion, distrust)
     - Cascading false positives, depending on self-reporting or testing
   - Combination may contribute to exit strategy
     - Cannot be taken for granted

issues

3. Can we protect fundamental rights by design?
   - Data Protection by Design and Default aims to protect against ALL fundamental rights infringements, NOT just violations of the GDPR
   - Data minimisation, purpose limitation, storage limitation, security by design

distinctions

- Manual, digital (combinations)
- Decentralisation (power) and distribution (storage)
- Based on testing, on self-identification, or a doctor's diagnosis
- Compulsory or voluntary (use of the APP)
- Constraint at iOS level, at APP level
- Open source or proprietary
- Access by GAPPLE, by APP provider, by governments
- Easy to repurpose (business model) or centralise (public security) or not
- Resilient against various types of attack or not
- Scale of surveillance that is enabled

Law, code and ethics

Legal constraints:

- If data is personal data (pseudonymous) GDPR applies
  - Legal basis: consent, contract (employment), vital interests, legislation, public task, legitimate interest of the app provider, see art. 6 GDPR
  - If health related: specific exceptions in art. 9 GDPR
  - Requirements: purpose limitation, data minimisation, storage limitation
- Most probably ePrivacy Directive applies
  - Explicit consent required whether personal data or not

Law, code and ethics

Legal constraints:

- If GDPR applies DPbDD and DPIA would normally apply
- Emergency legislation can exclude applicability of either or both
- Otherwise:
  - Data minimisation must be built-in by design
  - An assessment of risks to fundamental rights infringements
  - Such risks require mitigation or abstinence

Law, code and ethics

Code:

- What about protection by design of privacy, against discrimination, unwarranted surveillance, security risks?
  - Constraints to achieve data minimisation:
    - At iOS level (Big Tech deciding who has access to locally stored data)?
    - At app level (dependent upon applicable jurisdiction)?
    - Individual choice? (to download, install or deinstall app; to share data)
    - Choice architecture decided by Big Tech or APP developers?
    - Decision of legislator? (legitimate aim, safeguards, necessity, proportionality)

Law, code and ethics

Ethics:

- What about protection by design of privacy, against discrimination, unwarranted surveillance, security risks?
  - Constraints to achieve data minimisation:
    - At iOS level (Big Tech deciding who has access to locally stored data)?
    - At app level (dependent upon applicable jurisdiction)?
    - Individual choice? (to download, install or deinstall app; to share data)
    - Choice architecture decided by Big Tech or APP developers?
    - Decision of legislator? (legitimate aim, safeguards, necessity, proportionality)

Jurisdiction: law and rule of law

Who get to decide what choice end-users have?

- Depends on national and international jurisdiction
- In a constitutional democracy this depends on interplay executive and parliament
- Rule of law refers to contestability of decision-making in a court of law
  - Testing against international human rights law
  - Even emergency legislation requires safeguards (e.g. sunset clauses)

Joint Statement > 300 scientists 19 April

"Though the effectiveness of contact tracing Apps is controversial, we need to ensure that those implemented preserve the privacy of their users, thus safeguarding against many other issues, noting that such Apps can otherwise be repurposed to enable unwarranted discrimination and surveillance."

as signed by Mireille

Joint Statement > 300 scientists 19 April

"To aid the development of contact tracing without a centrally controlled database that holds private information on individuals,

- **Google and Apple are developing infrastructure to enable the required Bluetooth operations in a privacy protective manner**.
- Teams building the privacy protective schemes fully support this effort as **it simplifies—and thus speeds up—the ability to develop such Apps**.
- We applaud this initiative and caution against collecting private information on users.
- ***Some who seek to build centralized systems are pressuring Google and Apple to open up their systems to enable them to capture more data***."

as signed by Mireille

Joint Statement > 300 scientists 19 April

- "When multiple possible options to implement a certain component or functionality of the app exist, then **the most privacy-preserving option must be chosen**. Deviations from this principle are only permissible if this is necessary to achieve the purpose of the app more effectively, and must be clearly justified with sunset provisions.
- The use of contact tracing Apps **and the systems that support them must be voluntary**, used with the explicit consent of the user and the systems must be designed to be able to be switched off, and all data deleted, when the current crisis is over."

as signed by Mireille

Trace Together

- https://www.tracetogether.gov.sg
- One of the first, Singapore
- Bluetooth tracking, access to phone data by Health Ministry
- But had to keep phone unlocked
- Very low uptake, did not stop need for lockdown
- Emphasis on investment in both human and digital tracking

PEPP-PT

- https://www.pepp-pt.org
- Supposedly privacy by design, but unclear which industry partners partake
- Open to both centralised and decentralised deployment
- Not as transparent as claimed, many partners left

DP-3T

- https://github.com/DP-3T
- Decentralised in part, local storage
- Anonymous data? Depends on access of API provider
- Favours alerting only to confirmed infection (by doctor)
- No location data shared
- No access for government or healthcare or employers (depending?)
- Voluntary download & install (what if required for access to buildings?)

NHSX

- https://www.nhsx.nhs.uk/blogs/digital-contact-tracing-protecting-nhs-and-saving-lives/
- Centralised: data is collected by NHS and analysed before alerting?
- Based on unverified self reporting
- Rejection of GAPPLE API (which means working around various inconveniences, such as a drain on battery life)
- Note that the NHS is collaborating with Palentir

NHSX

"In future versions of the app, Gould suggested users could be asked to contribute additional data — such as their location — in order to help epidemiologists identify infection hot spots, while emphasizing that such extra contributions would be voluntary.

"The app will iterate. We've been developing it at speed since the very start of the situation but the first version that we put out won't have everything in it that we would like," he said. "We're quite keen, though, that subsequent versions should give people the opportunity to offer more data if they wish to do so."

TechCrunch 28 April 2020

NHSX

"The committee also asked Gould directly whether UK spy agency, GCHQ, was involved in the decision to choose a centralized approach for the app. The BBC reported yesterday that experts from the cyber security arm of the spy agency, the National Cyber Security Centre (NCSC), had aided the effort.

At first pass Gould dodged the question. Pressed a second time he dodged a direct answer, saying only that the NCSC was "part of the discussions in which we decided to take the approach that we've taken".

"[The NCSC] have, along with a number of others – the Information Commission's Office, the National Data Guardian, the NHS – been advising us. And as the technical authority for cyber security I'm very glad to have had the NCSC's advice," he also said."

TechCrunch 28 April 2020

NHSX

"During the committee hearing, Gould was also pressed on what will happen to data sets uploaded to the central server once the app has been required. He said such data sets could be used for "research purposes".

"There is the possibility of being able to use the data subsequently for research purposes," he said. "We've said all along that the data from the app – the app will only be used for controlling the epidemic, for helping the NHS, public health and for research purposes.

If we're going to use data to ask people if we can keep their data for research purposes we will make that abundantly clear and they'll have the choice on whether to do so."

TechCrunch 28 April 2020

NHSX

"Gould followed up later in the session by adding that he didn't envisage such data-sets being shared with the private sector. "This is data that will be probably under the joint data controllership of DHSC and NHS England and Improvement. I see no context in which it would be shared with the private sector," he said, adding that UK law does already criminalize the reidentification of anonymized data."

"In another exchange during the session Gould told the committee the app will not include any facial recognition technology. Although he was unable to entirely rule out some role for the tech in future public health-related digital coronavirus interventions, such as related to certification of immunity.."

TechCrunch 28 April 2020

Julie Cohen
@julie17usc

This is a five-alarm fire, folks. Lede should be "Controversial Tech Firm with Ties to Far Right and Shoddy Data Security in Talks with Federal And State Authorities to Develop Covid-19 Tracking App"
gizmodo.com/creepy-face-re...
engadget.com/clearview-ai-s...

> **Elizabeth Joh** @elizabeth_joh · 14h
> THIS AIN'T IT FRIENDS

19:55 · 29/04/2020 · Twitter Web App

GAPPLE API

You Retweeted

Thierry Breton ✓
@ThierryBreton

I just had a good exchange with #Apple CEO @tim_cook on the need to ensure that contact tracing apps are fully:
✓ anonymised
✓ voluntary
✓ transparent
✓ temporary
✓ secured
and interoperable across operating systems and borders.

#Deconfinement apps must respect our #privacy.

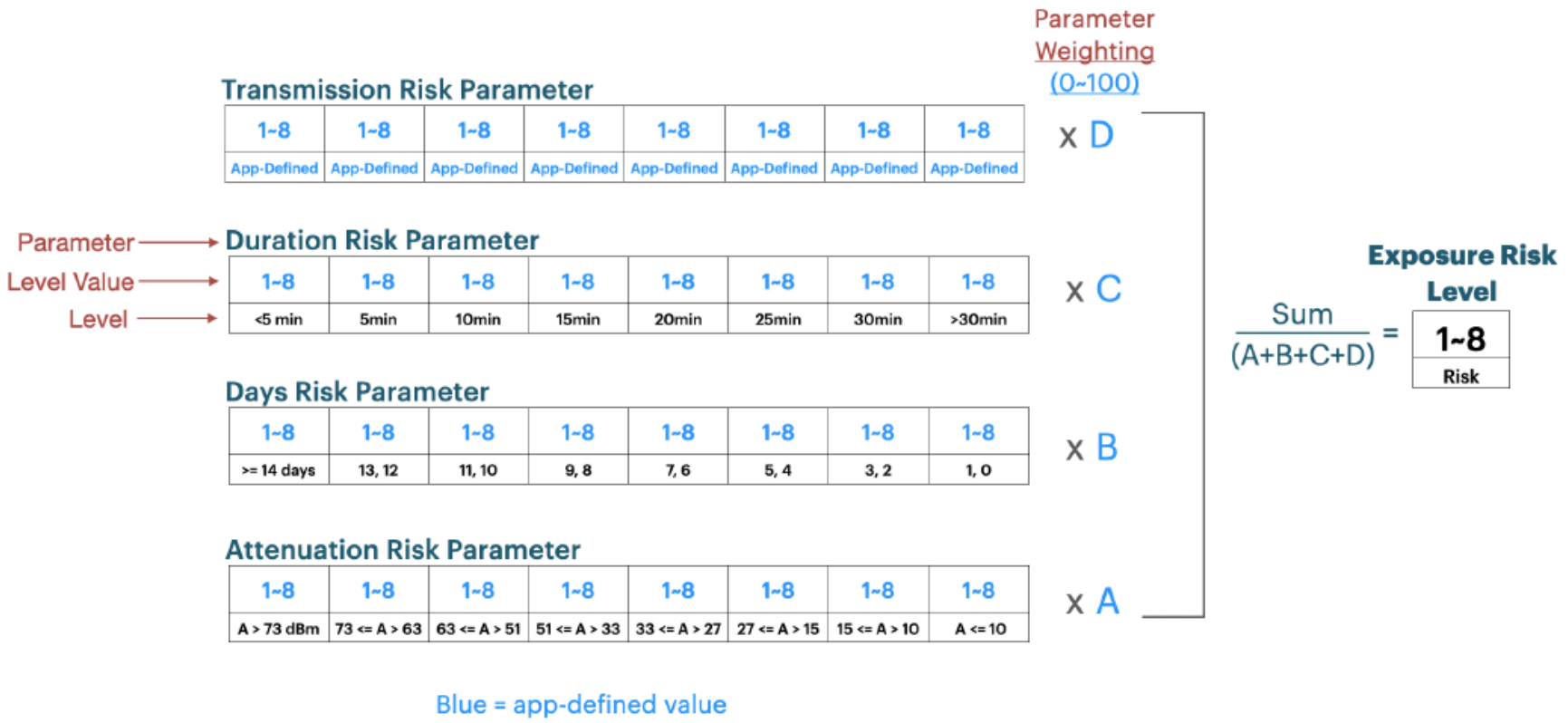
ENExposureConfiguration

Overview

Contains configuration parameters for exposure detection.

Discussion

The following diagram illustrates the data structure and formula used to calculate the Exposure Risk Level.



GAPPLE API

- APPLE: Cha, a senior strategist of the health care division; Ron Huang, head of Apple's location services group; Dr. Guy "Bud" Tribble, internally known as the "privacy czar"; cryptographers Yannick Sierra and Frederic Jacobs (Jacobs has been credited for helping create the secure messaging app Signal).

- GOOGLE: Yul Kwon, a senior director for the company and a former deputy chief privacy officer at Facebook; Ronald Ho, Senior product manager, who works on Bluetooth and connectivity efforts

- Early connections with MIT's PACT and Europe's DP-3T

GAPPLE API

- https://www.apple.com/covid19/contacttracing
- not an APP but an API: a set of specifications that public health organizations can tap into to build their own contact tracing apps
- the API will be built into the iOS
- once Bluetooth is turned on and the user opts in the phone sends anonymous little chirps that other phones can listen into (Apple's API means the app can continue to send these chirps out even if it's not running in the foreground at the time)

GAPPLE API

- DP-3T idea of using rotating codes has been integrated: apps will broadcast a cryptographic key that changes randomly, while they monitor other nearby phones.
- when user reports a Covid-19 diagnosis, the app will upload the cryptographic keys that were used to generate the codes from the past few weeks onto a server.
- all other apps (in the region?) download those keys, check matches with stored codes of infected persons.

GAPPLE API

- Constraining ability of APP developers to collect data for central databases
- Precludes access to Bluetooth IDs (on phone)
- **Is this protection by design and/or legal protection by design?**

Note:

- May create **a new monopoly** for access to the Bluetooth IDs
- With far reaching consequences for **public and private surveillance**

references

- Romain Dillet, 'Hundreds of French Academics Sign Letter Asking for Safeguards on Contact Tracing', TechCrunch (blog), 27 April 2020, https://social.techcrunch.com/2020/04/27/hundreds-of-french-academics-sign-letter-asking-for-safeguards-on-contact-tracing/
- Farr, Christina. 'How a Handful of Apple and Google Employees Came Together to Help Health Officials Trace Coronavirus'. CNBC, 28 April 2020. https://www.cnbc.com/2020/04/28/apple-iphone-contact-tracing-how-it-came-together.html.
- Leswing, Kif. 'Apple and Google Release Test Version of Coronavirus Tracing Software'. CNBC, 29 April 2020. https://www.cnbc.com/2020/04/29/apple-and-google-release-test-version-of-coronavirus-tracing-software.html.
- Kieren McCarthy, 'UK Snubs Apple-Google Coronavirus App API, Insists on British Control of Data, Promises to Protect Privacy', accessed 1 May 2020, https://www.theregister.co.uk/2020/04/28/uk_coronavirus_google_apple_api/

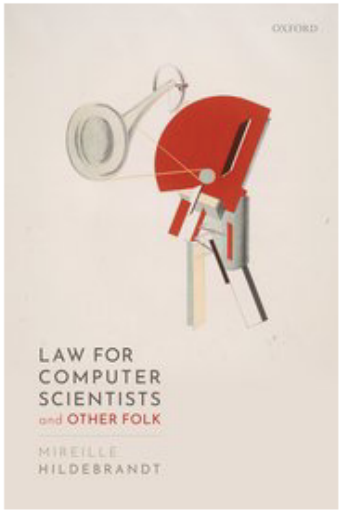
references

- Alfred Ng, 'Tech Isn't Solution to COVID-19, Says Singapore Director of Contact Tracing App', CNET, accessed 1 May 2020, https://www.cnet.com/news/director-behind-singapores-contact-tracing-app-says-tech-isnt-the-solution-to-covid-19/
- Samuel Stolton, 'Digital Brief: PEPP-PT - The Inside Story', Www.Euractiv.Com (blog), 23 April 2020, https://www.euractiv.com/section/digital/news/digital-brief-pepp-pt-the-inside-story/

On relevant data protection law:

LSTS repository https://lsts.research.vub.be/en/data-protection-law-and-the-covid-19-outbreak

Gabriela Zanfir-Fortuna on Future of Privacy Forum https://fpf.org/2020/04/30/european-unions-data-based-policy-against-the-pandemic-explained/



Law for Computer Scientists and Other Folk

Mireille Hildebrandt

- The only dedicated textbook introducing law to computer scientists and other relevant audiences (non lawyers)
- Dedicated focus on cybercrime, intellectual property, data protection, private law liability and legal personhood
- The book will provide insight into the operations of the law, demonstrating the specifics of legal reasoning
- Clear structure with a reader's guide, a handy glossary/index, and frequent cross-referencing throughout the book
- This is an open access title available under the terms of a CC BY-NC-ND 4.0 International licence

£29.95

Add to Cart

Paperback

Published: 23 April 2020 (Estimated)

352 Pages

234x156mm

ISBN: 9780198860884

Also Available As:

Hardback

Ebook

Bookseller Code (AE)

the eBook will soon be available in open access at OUP