

If at first you don't succeed

NORWAY'S TWO CONTACT TRACING APPS

Eivind Arvesen

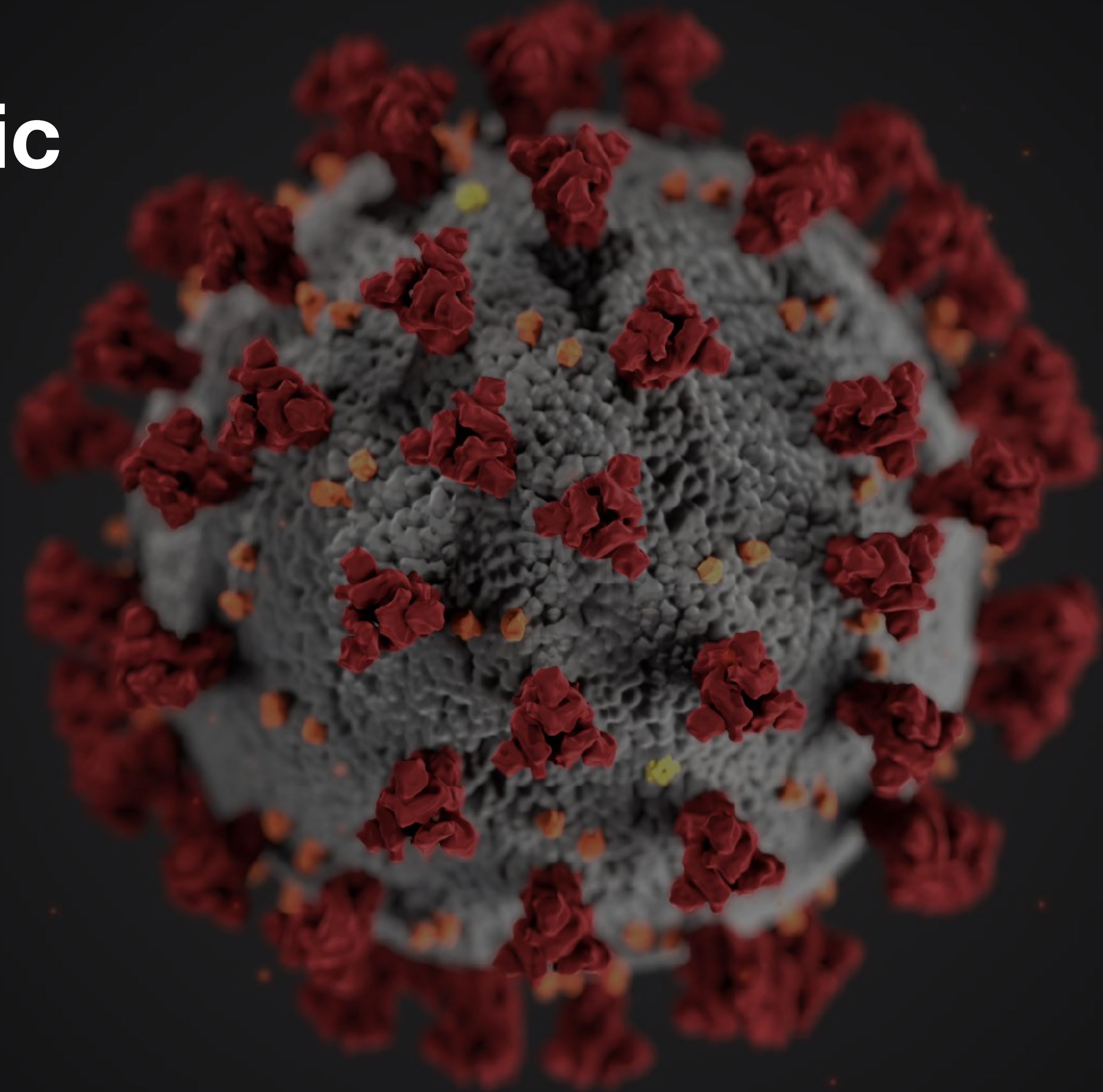
 @EivindArvesen

Conference on Privacy Engineering Practice and Respect (PEPR)

June 11th 2021

Background

Pandemic





Background

Contact tracing

- Interview infected
 - Who were they in contact with during their infectious period?
 - Tell the contact to isolate and get tested.
- Resource intensive

***We have sensing supercomputers in our
pockets most of the time!***

A blue surgical mask with white elastic straps is positioned on the left side of the image. To its right is a yellow book cover. The text "There's an app for that!" is written in white on the mask, and "COVID-19" is written in black on the book cover.

There's an app for that!

COVID-19

The first app

The first app

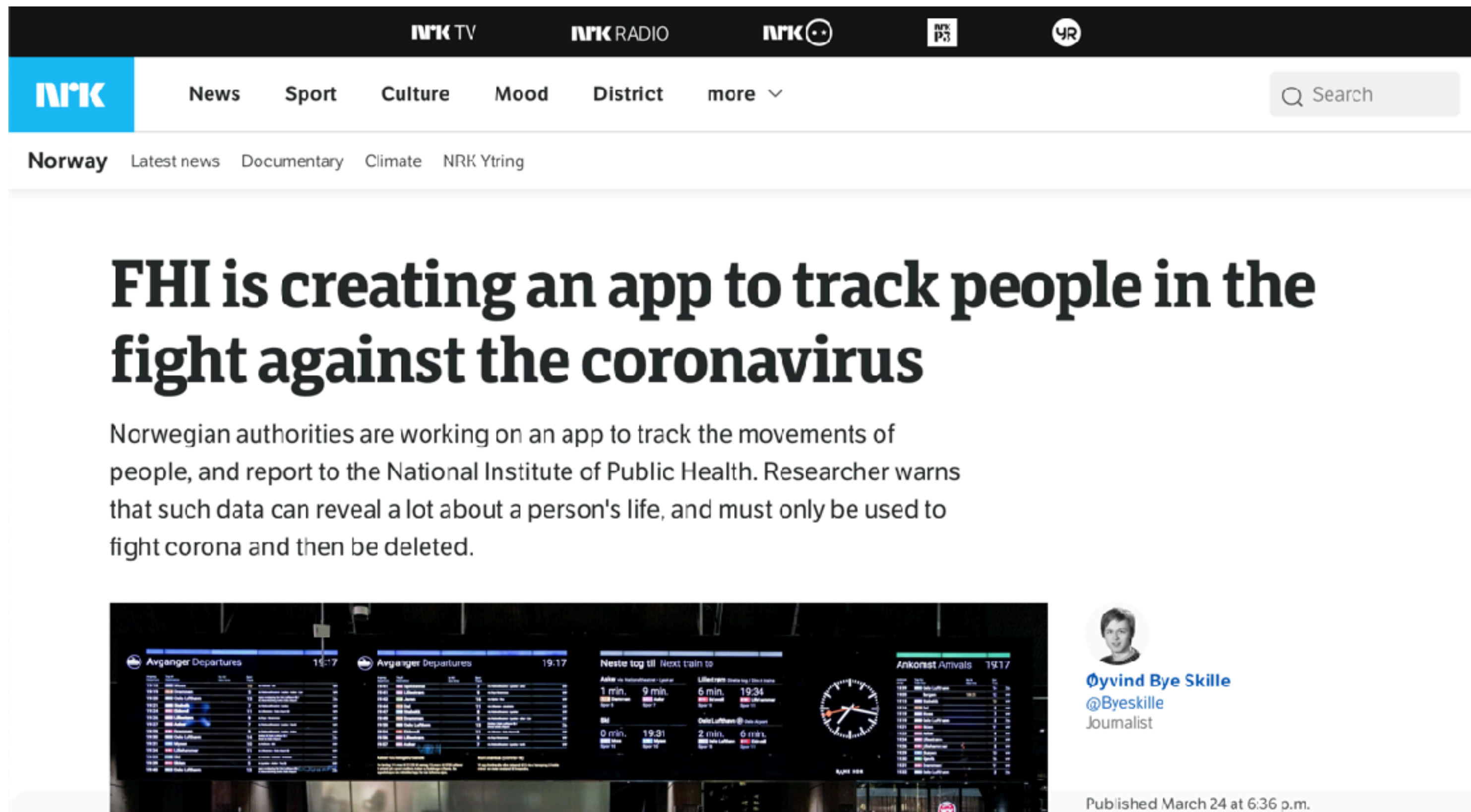
Summary

- Bluetooth & Location data
- Centralized storage
- Closed source
- Multiple purposes
- Required registration (de facto identification)
- Multiple issues – including use of a static, device-specific identifier



The first app

Public introduction: Source code leak



The screenshot shows the NRK website interface. At the top is a navigation bar with logos for NRK TV, NRK RADIO, NRK (with a smiley face icon), NRK P3, and YR. Below this is a secondary navigation bar with the NRK logo, links for News, Sport, Culture, Mood, District, and a 'more' dropdown menu, followed by a search bar. A third bar contains links for Norway, Latest news, Documentary, Climate, and NRK Ytring. The main content area features a large headline: 'FHI is creating an app to track people in the fight against the coronavirus'. Below the headline is a sub-headline: 'Norwegian authorities are working on an app to track the movements of people, and report to the National Institute of Public Health. Researcher warns that such data can reveal a lot about a person's life, and must only be used to fight corona and then be deleted.' There is an image of a train station departure board. To the right of the image is a profile for Øyvind Bye Skille, a journalist, with his Twitter handle @Byeskillen. At the bottom right, it says 'Published March 24 at 6:36 p.m.'

FHI is creating an app to track people in the fight against the coronavirus

Norwegian authorities are working on an app to track the movements of people, and report to the National Institute of Public Health. Researcher warns that such data can reveal a lot about a person's life, and must only be used to fight corona and then be deleted.

Øyvind Bye Skille
@Byeskillen
Journalist

Published March 24 at 6:36 p.m.

- If you collect large amounts of location data about an individual, it is unlikely that the data will be considered anonymous. It is more likely that this will be considered as data about an identifiable individual, and thus as personal information, says Bentzen, who believes that information about someone who is infected is even more sensitive because it is health information.

- For those who are trying to find out about the infection, it is probably useful to have as much information as possible about the population and thus collect a lot. How should it be assessed against privacy?

- You can not collect more data than necessary to prevent infection, for example because you think it would be nice to have additional data available for research in the future, the researcher answers.

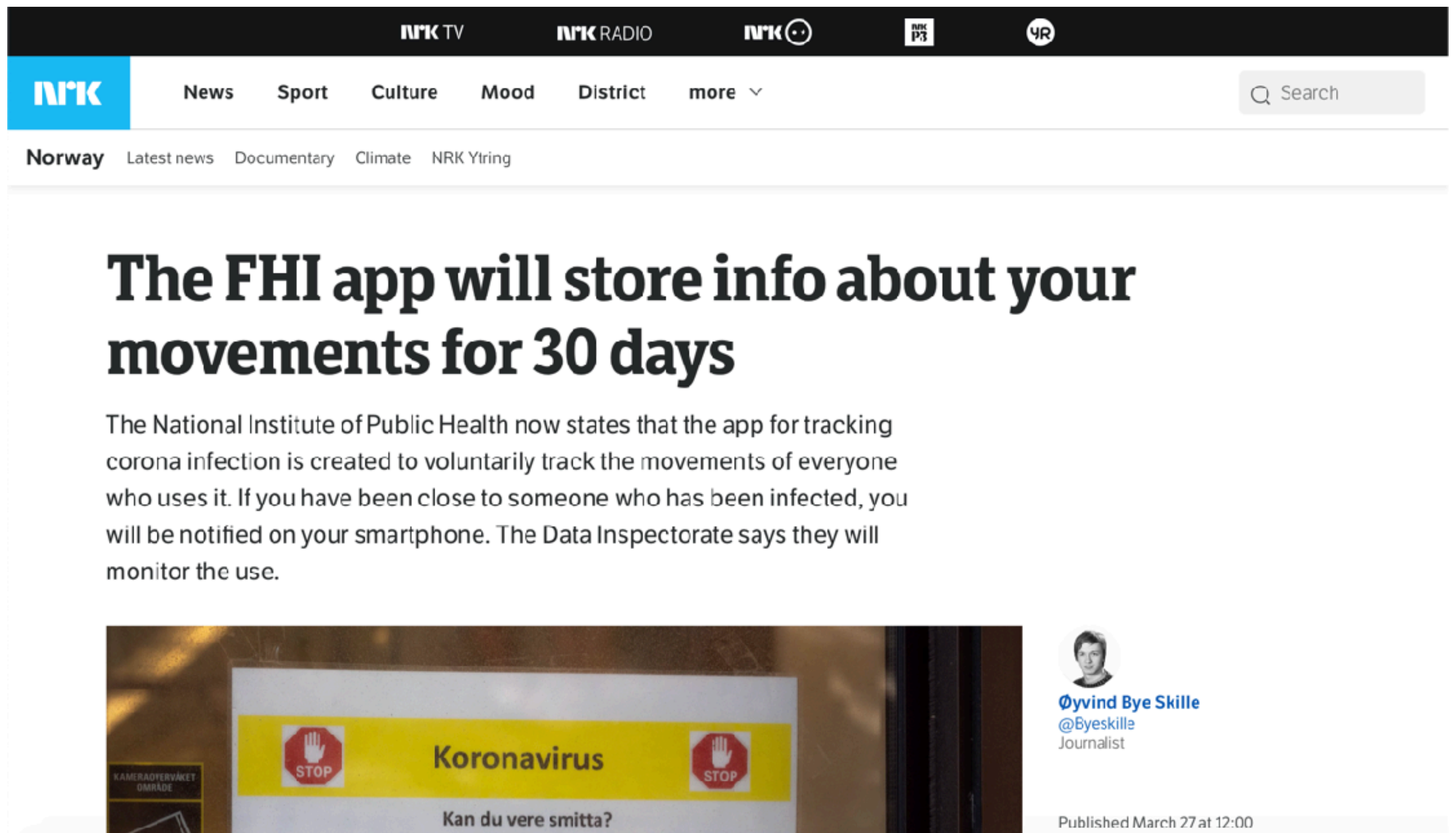
The first app

Public introduction: Source code leak

The app will be voluntary to install, and will then collect the movements of the mobile user to a central database.

- Once the app is installed, it will collect data using GPS and Bluetooth. The data is then encrypted and stored in a separate secure cloud solution. If a user is found to be infected with the virus, it will be possible to track the phones that have been in close contact with the infected person in the last 14 days, writes Simula who creates the app on his website.

This tracking and calculation must be done in the computer systems of the authorities.



The screenshot shows the NRK website's news section. The header includes the NRK logo and navigation links for TV, Radio, and various content categories. The main headline reads: "The FHI app will store info about your movements for 30 days". Below the headline, a sub-headline states: "The National Institute of Public Health now states that the app for tracking corona infection is created to voluntarily track the movements of everyone who uses it. If you have been close to someone who has been infected, you will be notified on your smartphone. The Data Inspectorate says they will monitor the use." At the bottom of the article preview, there is a photograph of a yellow sign with the word "Koronavirus" and two red stop signs. To the right of the image is a profile picture of Øyvind Bye Skille, a journalist, and a timestamp indicating the article was published on March 27 at 12:00.

The FHI app will store info about your movements for 30 days

The National Institute of Public Health now states that the app for tracking corona infection is created to voluntarily track the movements of everyone who uses it. If you have been close to someone who has been infected, you will be notified on your smartphone. The Data Inspectorate says they will monitor the use.

Koronavirus

Kan du vere smitta?

Øyvind Bye Skille
@Byeskillen
Journalist

Published March 27 at 12:00

The first app

A rough timeline

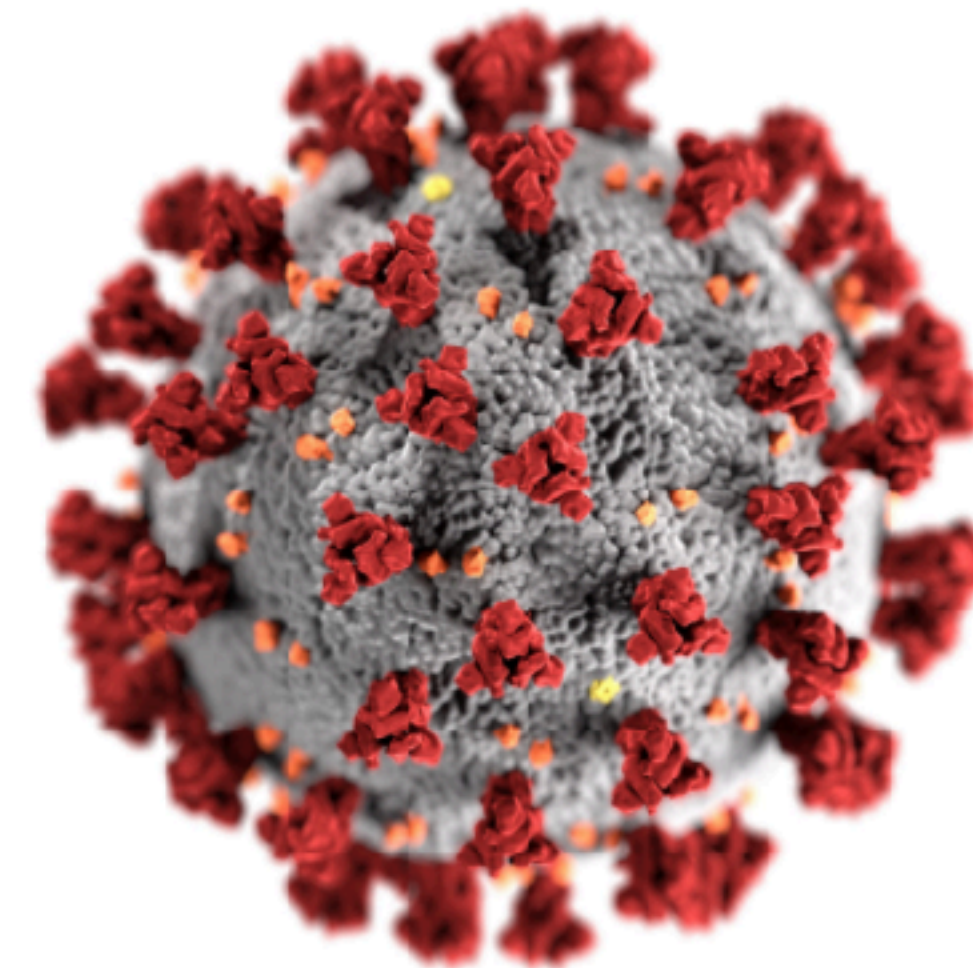
- Highly criticized from get-go
- Over 300 tech-professionals launched petition to change approach
- Government appointed expert group concludes neither security nor privacy is handled responsibly
- Supplier handled any criticism by public attacks
- Negative user feedback from battery-drain, inability to register, limited notification support at launch

Joint statement on contact tracing for Norway



Joint Statement Norway
May 19 · 13 min read

[Follow](#)



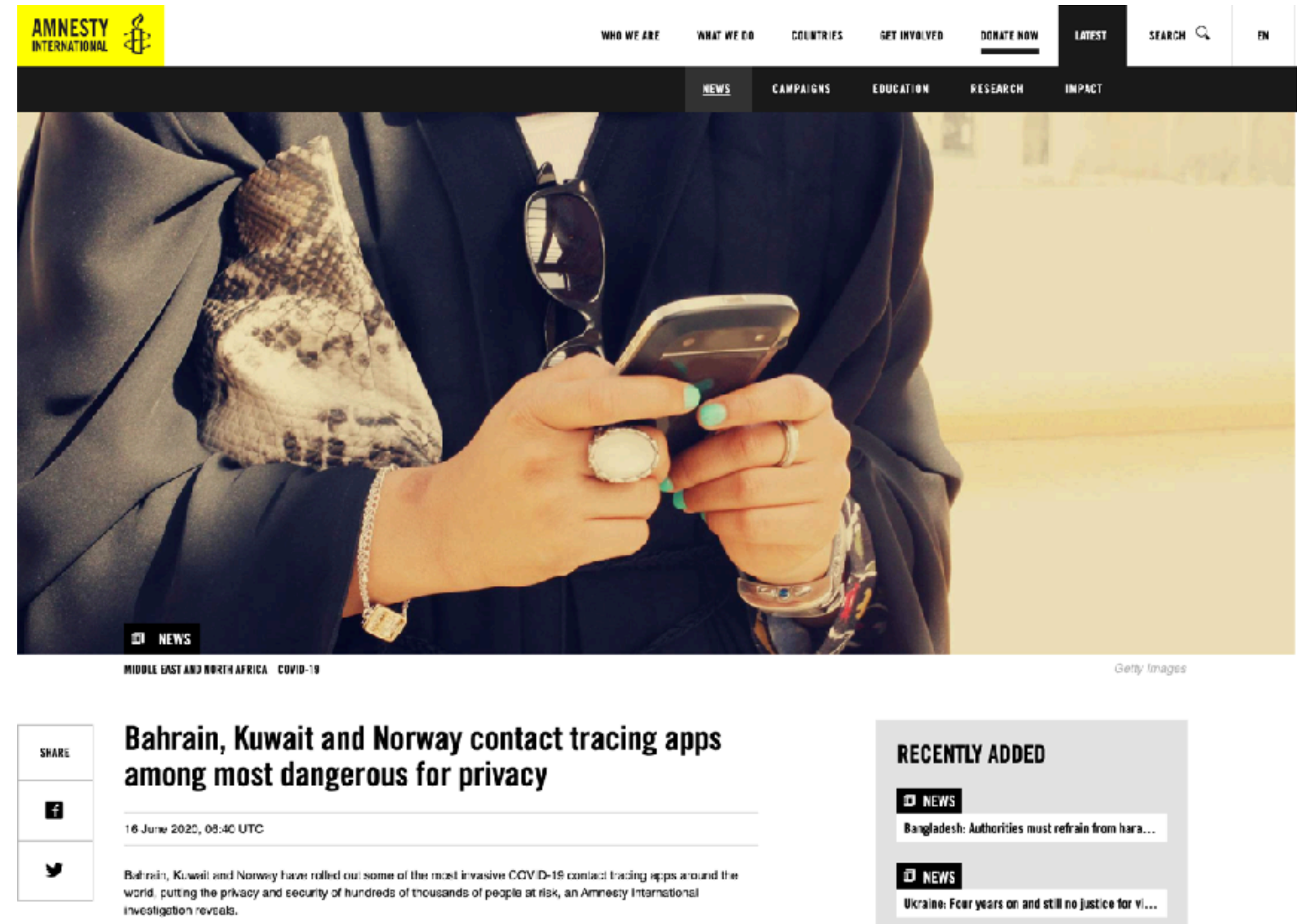
Coronavirus (Source: [CDC](#))

Echoing the statement¹ signed by hundreds of scientists and researchers from across the globe, this statement reflects the view of the undersigned Norwegian technology, security and privacy experts. It is the result of many discussions, where we sought to balance important requirements and values. Our main goal has been to contribute with a unifying, realistic and constructive proposal. We believe this proposal shows a path that answers substantial concerns, and outlines a solution that will receive public support.

The first app

A rough timeline

- Parliament: «Split purpose by consent!»
- Amnesty International stated that the app was among the most dangerous contact tracing apps for privacy.
- International media attention (New York Times, The Guardian, etc.)
- Norwegian Data Protection Authority declared data processing forbidden



The second app

The second app

Summary

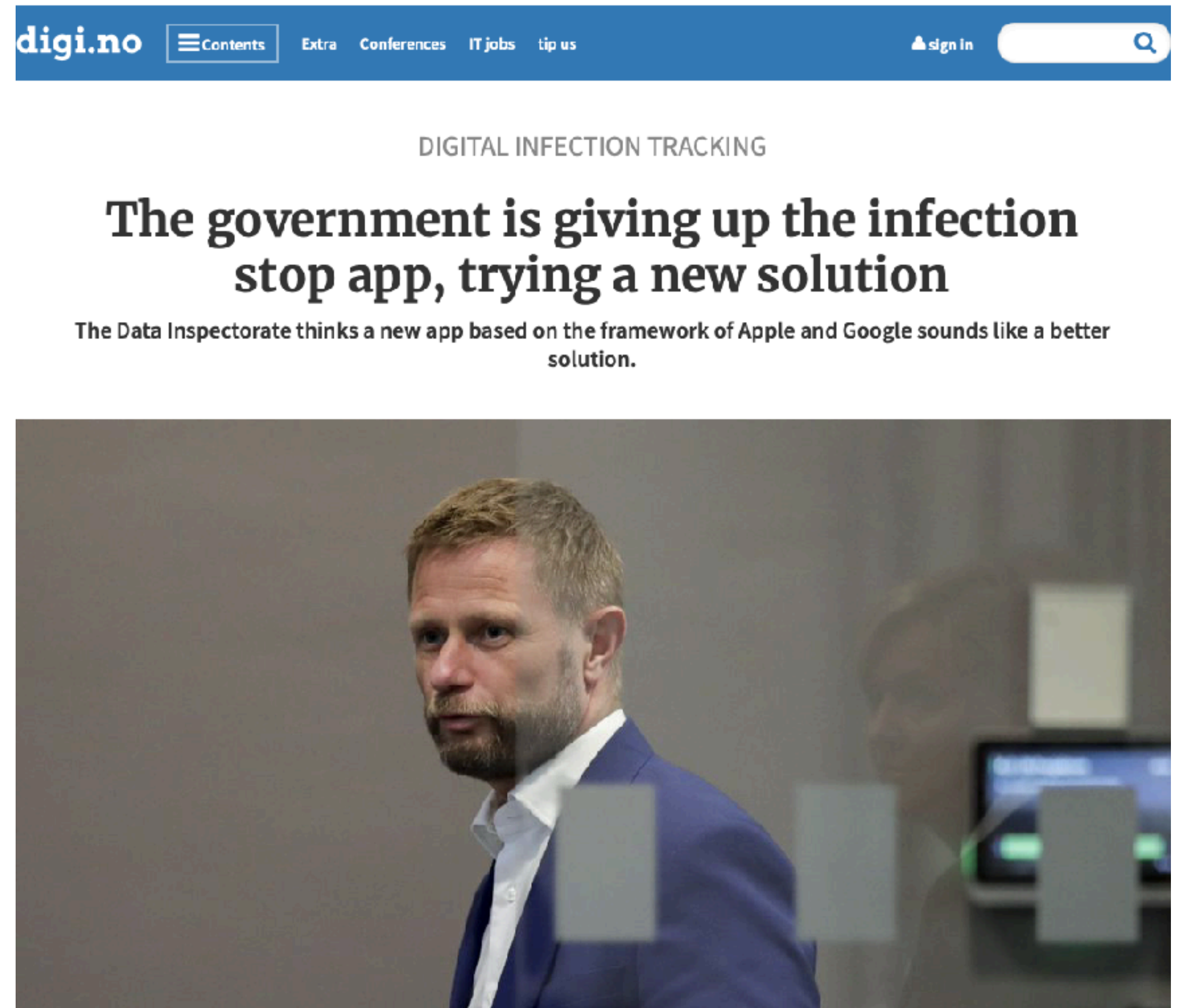
- Bluetooth only
- Decentralized storage
- Open source
- Single purpose



The second app

A rough timeline

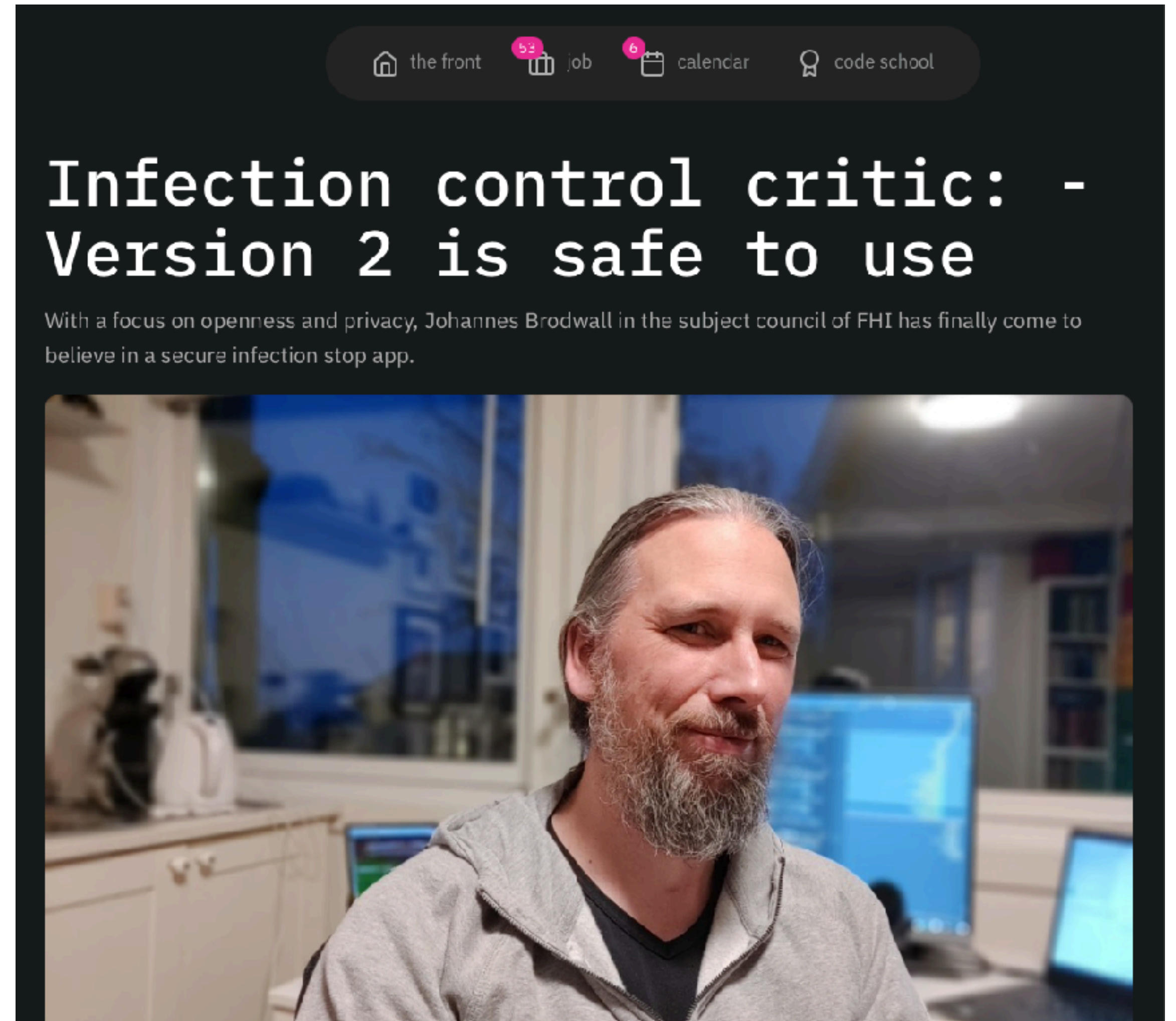
- Open source code; accepting contributions
- External council as community representatives
- Open Slack for feedback and discussions



The second app

A rough timeline

- Vocal critics of the first app spoke out, vouching for the new app
- Large ad-campaigns, including targeted toward non-native speakers and vulnerable populations
- Launch: Positive user experience and public reaction



Comparison

Comparison

Privacy-related qualities

	Sensor data	Basis for processing	Purpose for processing	Data collected	Who accesses data	Where is data stored	Privacy Framework
First app	Bluetooth, GPS	Regulation	Contact tracing, evaluating restrictions, producing research data	Phone number, location, contacts, analytics, diagnostics/telemetry	Health officials, developers	Central data store / Public cloud	
Second app	Bluetooth	Consent	Contact tracing	Contacts	Health officials	Decentralized / User's device	Apple/Google Framework

Comparison

Privacy-related qualities

	Sensor data	Basis for processing	Purpose for processing	Data collected	Who accesses data	Where is data stored	Privacy Framework
First app	Bluetooth, GPS	Regulation	Contact tracing, evaluating restrictions, producing research data	Phone number, location, contacts, analytics, diagnostics/telemetry	Health officials, developers	Central data store / Public cloud	
Second app	Bluetooth	Consent	Contact tracing	Contacts	Health officials	Decentralized / User's device	Apple/Google Framework

Comparison

Privacy-related qualities

	Sensor data	Basis for processing	Purpose for processing	Data collected	Who accesses data	Where is data stored	Privacy Framework
First app	Bluetooth, GPS	Regulation	Contact tracing, evaluating restrictions, producing research data	Phone number, location, contacts, analytics, diagnostics/telemetry	Health officials, developers	Central data store / Public cloud	
Second app	Bluetooth	Consent	Contact tracing	Contacts	Health officials	Decentralized / User's device	Apple/Google Framework

Comparison

Privacy-related qualities

	Sensor data	Basis for processing	Purpose for processing	Data collected	Who accesses data	Where is data stored	Privacy Framework
First app	Bluetooth, GPS	Regulation	Contact tracing, evaluating restrictions, producing research data	Phone number, location, contacts, analytics, diagnostics/telemetry	Health officials, developers	Central data store / Public cloud	
Second app	Bluetooth	Consent	Contact tracing	Contacts	Health officials	Decentralized / User's device	Apple/Google Framework

Comparison

Privacy-related qualities

	Sensor data	Basis for processing	Purpose for processing	Data collected	Who accesses data	Where is data stored	Privacy Framework
First app	Bluetooth, GPS	Regulation	Contact tracing, evaluating restrictions, producing research data	Phone number, location, contacts, analytics, diagnostics/telemetry	Health officials, developers	Central data store / Public cloud	
Second app	Bluetooth	Consent	Contact tracing	Contacts	Health officials	Decentralized / User's device	Apple/ Google Framework

Comparison

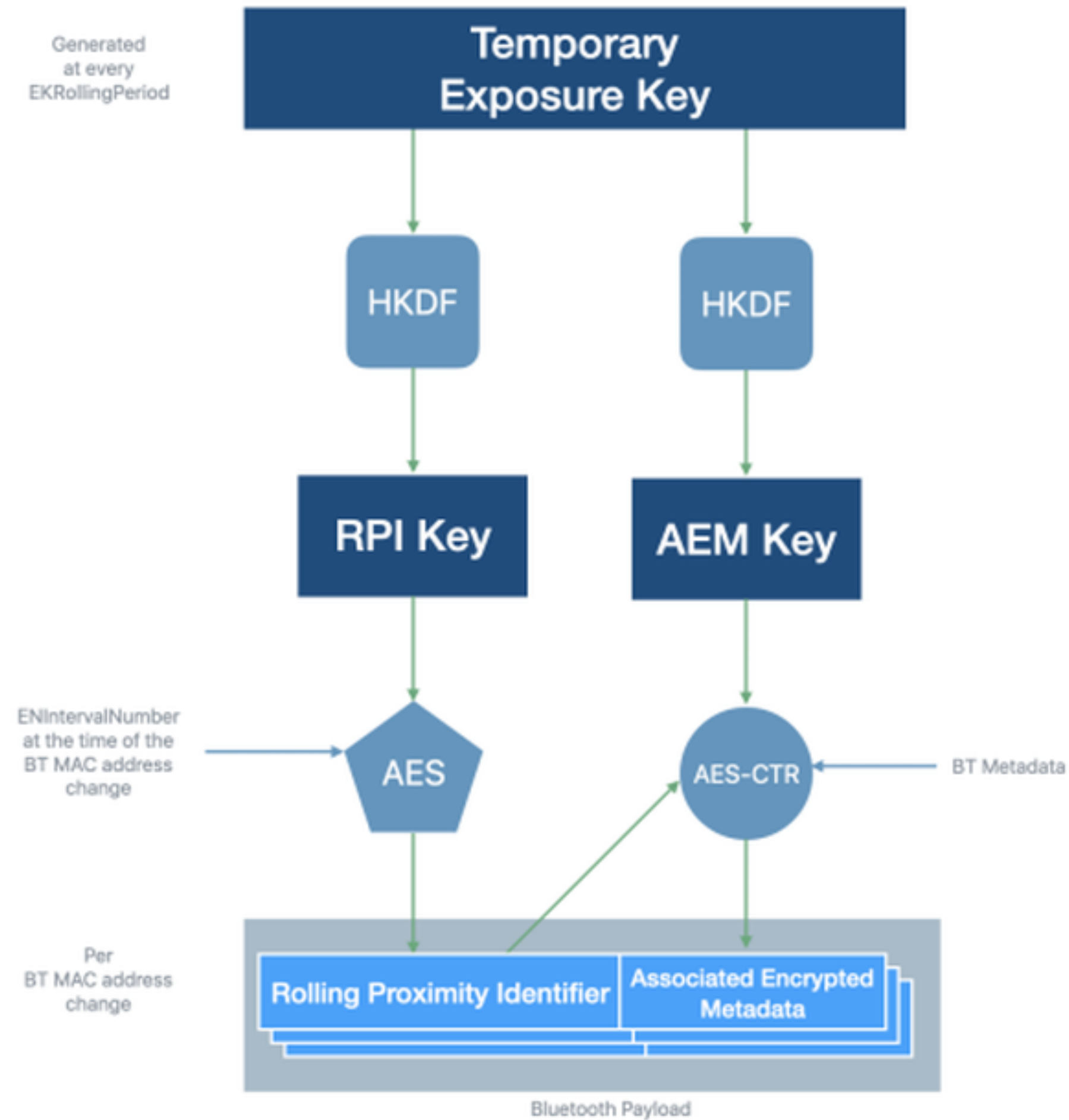
Re: «necessity» of GPS and central data storage

- Platform limitations around background Bluetooth-usage in early 2020
- Singapore (creative hack around limitations without compromising on privacy!)
- Various other countries (different configurations... convergence)
 - Common European guidelines
 - EU commission's recommendations on apps for contact tracing
 - EU resolution on coordinated work against COVID-19
 - Guidelines from the European Data Protection Board (EDPB)
- DP-3T (open, decentralized anonymous contact tracing protocol)
- GAEN (requirements)

Comparison

App 2

Key Schedule for Exposure Notification



Comparison

App 1

Persistent device-specific identifier

Comparison

Known risks

The first app

- Cannot specify exceptions to data sharing
- Police access to BLE-data?
- Data theft, leak or misuse
- Function creep
- Users are de facto identified
- Potentially fingerprintable analytics
- No data interoperability in EU
- SMS for notifications
- Data deletion also deleted audit logs
- Quality issues in contact analysis code
- Anonymization process for long term research data not complete
- Lack of transparency (source code; communications re: purpose(s), data use and «anonymization»)

The second app

- Cannot specify exceptions to data sharing
- Trusting Google and Apple to not do anything else with or somehow exfiltrate the locally stored data

Comparison

Known vulnerabilities

The first app

- Identification, tracking and impersonation of users
- ...

The second app

- Health authorities have a theoretical possibility of identifying uploaders (by correlating between logs)
- Third party correlation attacks
- Replay attacks
- Cross-correlated mapping attacks

Conclusion

Conclusion

GDPR (art. 5): Principles relating to processing of personal data

	App 1	App 2
Lawfulness, fairness and transparency	✗	✓
Purpose limitation	✗	✓
Data minimization	✗	✓
Accuracy	?	?
Storage limitation	✗	✓
Integrity and confidentiality (security)	✗	✓
Accountability	✗	✓



NORWAY

**GRATUITOUS
DATA COLLECTION**

IS THIS PRIVACY?

Conclusion

Take-aways

- You don't want to be in a position of solving difficult, novel problems in a crisis – using tools that were not built with this purpose in mind!
- Involve privacy and security experts in developing high risk engineering solutions
- Good technology respects its users, as well as their interests and rights
- Even a major pandemic is no reason to lower privacy standards

Conclusion

Take-aways

- We need to work toward objective rules and metrics, and cement privacy engineering as an established field with agreed-upon principles... and make it part of general software engineering knowledge.

Thanks!

eivind.arvesen@gmail.com

 @EivindArvesen

<https://www.eivindarvesen.com>