Handshake

Track your proximity to COVID-19.

Further thoughts on implementation

Overview of design choices

This basic implementation uses a hash of a user's email and a passphrase to aid privacy (or just a unique phrase), a centralised data store (Google Sheets), decentralised 'logins', is a web-page and uses only free tools.

This website/set up was **simple to create**, it wouldn't be too hard for anyone with some resources to create an improved version.

It does not rely upon users installing any apps, making it easily accessible.

It does not rely upon users sharing their location history or bluetooth data.

Privacy

Privacy is still an issue that would need to be tackled. Using a unique privacy passphrase and then hashing people's email addresses with it (or hashing a unique phrase) is possibly a bit helpful, but it does nothing to protect you from people you Handshake with that might want to reveal your identity. Plus, I'm not a cryptography or privacy expert so can give no guarantees around the privacy of this system whatsoever.

A privacy passphrase is added to the users email before hashing (using SHA-256) so that a person with a lot of email addresses can't just hash all the email addresses in their directory to match with publicly available data.

The option is given to use just a unique phrase that gets hashed and it is hoped that no two users come up with the identical unique phrase but this offers slightly more privacy as users don't need to volunteer their email address to the Handshake webpage
And it makes very clear that users *won't* get email notifications from that page (since in this particular implementation of the handshake idea, email notifications are not possible - though it could be extended to).
To generate the same hash using the unique phrase version a user with the email "test@test.com" and password "OneTwoThree" would use "test@test.comOneTwoThree" as their unique phrase.

This idea would still work if the information volunteered was stored privately rather than made publicly available. The onus would then be on the organisation that controlled the data to properly analyse it and make that analysis available to the people who it would be helpful for.

Other comments

People do not need to log in to Handshake every time to generate a QR code, they can generate it once at the Generator then keep their static unique QR code for future use.

The use of Google forms and sheets as opposed to a database, while unorthodox, does make it easy to publicly share data in an append only manner, is free, and seems appropriate for this basic working version.

This does rely on trusting that people don't mess with Handshake by adding fake entries, but I am hopeful that this would not happen. Fully featured versions of Handshake could mitigate this in various ways I'm sure.

You can have QR codes for locations such as at each coffee table or train seat - generate them here. In the current implementation, QR codes should be displayed at locations and *scanned by people that visit them* (rather than having the location owner scan the QR code of the customer, for example).

The Handshake idea was partly inspired by Co-Epi.

Handshake replaces the somewhat dangerous practice (in these times) of physically shaking hands.

Future work ideas (just ideas, I am not in a position to work on them)

For the latest ideas, view the Github Project Board and the Github Issues .

For example:

- Create a push notification service
- Real-time visualisation
- Improve analysis of connection data

If you want to get involved

Get involved on GitHub

or

Send an email to get.involved.handshake@gmail.com