FreeFromCovid

OVERVIEW:

We want accelerate the revival of commerce and other aspects of social life after the world emerges from the COVID-19 (Coronavirus) threat.

As certain areas in the world emerge from "lock down" or "shelter in place", reports indicate that people are still reluctant to leave the house and business is still suffering.

Many countries around the world are increasing their rates of COVID-19 testing. In addition, various contact tracing applications are now implemented or soon will be implemented in various countries to help track and reduce the spread of COVID-19.

With this multitude of high-quality contact tracing applications, it will be difficult for third-parties to know which of these applications might be legitimate and capable of being trusted, especially across borders and across continents. In fact, it is likely that "fake" or "dummy" applications will surface, causing considerable confusion and continuing distrust.

This web-based application will provide an easy, secure, and private means to allow people to prove that they have recently been tested "negative" for coronavirus (i.e., that they are not a carrier of COVID-19), or that their legitimate contact tracing application does not reveal any relevant contacts, or both.

The app will prioritize:

- Privacy and security
- Speed and reliability
- Decentralization, with no single authority or point of failure
- Difficulty to falsify or forge app views and test results
- Ease and simplicity of use
- Fast implementation internationally and across borders
- Low cost and widely available means of use

The application will allow governmental entities to offer the service to their citizens, and to authorize only specific contact tracing applications to function as qualified verification methods.

The application can also be used by private entities, such as:

- Businesses who wish to prevent disease from spreading among their employees;
- Conference organizers to prevent disease from spreading among their attendees;

- Office buildings as a benefit to their tenants;

- Hotels and theaters as a means of assuring and ensuring the safety of their guests;

- Restaurants, cafes, bars, and nightclubs as a means of assuring and ensuring the safety of their patrons; and

- Other service providers as a means of assuring and ensuring the safety of their customers, patients, and clients.

DISTRIBUTION AND IMPLEMENTATION:

The source code repositories will be shared under the free and open source Mozilla Public License Version 2.0 to all governmental entities.

This will allow governmental entities to deploy the code on their own servers to ensure privacy and security, and to modify the code, if the governmental entity chooses to do so. This will also allow government entities to audit the code.

Businesses will also be allowed to host the application on their own servers, and modify the code, in exchange for a small license fee and limited license agreement.

In addition, the application will also be hosted on secure servers maintained by Incubator LLC, and offered as a free service to both governmental entities and businesses.

DESCRIPTION:

The application will have four different access points:

- Control Users

- Contact Tracing Applications

- Gatekeepers

- Persons

The application will function based upon a combination of:

(1) integrations with Contact Tracing Applications; and

(2) express and deliberate consent by users of the Contract Tracing Applications (collectively, "Persons") to share their COVID-19 status only on a highly directed and specific basis.

Control Users could be governmental entities that want to offer the application for their citizens, or private entities that wish to use the application for their own purposes.

Only Control Users will be able to authorize certain specific Contact Tracing Applications to integrate with the application.

Control Users and Contact Tracing Applications will have secure login access to the application. Encryption in transit, 2-Factor-Authentication, and password strength features will be mandated. Encryption at rest will be used in INCUBATOR LLC's deployment of the application, and strongly recommended for all other deployments.

Gatekeepers are third-parties who wish to know the Person's COVID-19 status – such as restaurants, hotels and resorts, conference facilities, government buildings, factory or assembly facilities, office buildings, and the like. Gatekeepers will not have accounts in this application. No information about any Gatekeeper or Gatekeepers will be collected, processed, or stored in this application in any way.

Persons are users of Contact Tracing Applications. Persons will not have accounts in this application. No information about any Person or Persons will be collected, processed, or stored in this application in any way.

1. Integrations With Contact Tracing Applications

When authorized by a Control User, a Contact Tracing Application would be provided with a secure account in this application.

The Contact Tracing Application will be allowed to log in to their account, obtain simple instructions for API integration, generate API keys, and refresh their API keys.

The Contact Tracing Application's access to this application would be locked to a specific IP address or domain of the Contact Tracing Application, and also secured by the API keys. All API traffic would occur over at least 256-bit SSL encryption.

A request will be initiated by a Person – i.e., the Contact Tracing Application's end user. The Person's request would be routed by the Contact Tracing Application's server to this application.

When a verified request is sent to this application by an authorized Contact Tracing Application, this application would return a signed URL. The signed URL would then be routed back to the Person – i.e., the Contact Tracing Application's end user.

When the signed URL is opened in a browser, a Quick Response (QR) code would appear on the Person's local device.

The signed URL link for this QR code would expire in 5 minutes. At the end of this limited time period, the signed URL and QR code would no longer be usable.

This QR code will be called a "Personal QR Code". The usage of Personal QR Codes is discussed later in this document.

As an example of an integration between this application and a Contact Tracing Application:

- The Contact Tracing Application would add a button in the User Interface (UI) of their on-device app. For example, this button could be called "Get QR Code", or "Confirm Me", or similar.

- When a Person – i.e., the Contact Tracing Application's user -- presses the on-device button, the on-device Contact Tracing Application would determine if its user has tested negative (verified as "no COVID-19"), and/or has not been in proximity with anyone who is a known carrier of COVID-19.

- If the on-device Contact Tracing Application shows that its user has tested positive (verified as being a "COVID-19 carrier"), and/or has been in proximity with anyone who is a known carrier of COVID-19, the Contact Tracing Application should present an error or other declination message to its user.

- If the on-device Contact Tracing Application shows that its user has tested negative (verified as "no COVID-19"), and/or has not been in proximity with any person who is a known carrier of COVID-19, the Contact Tracing Application's server would route the user's request to this application.

- This application would return a signed URL to the Contact Tracing Application's server.

- The signed URL would be relayed or routed by the Contact Tracing Application back to the Person who made the request.

- A browser would open on the local device of the Person and open the signed URL.

- The Personal QR Code from this application would appear in a browser tab on the Person's local device.

- The signed URL for the Personal QR Code would expire in 5 minutes.

2. Using the Personal QR Code

The Personal QR Code can be scanned by any modern mobile phone using a browser-based interface provided by this application. An individual who scans a Personal QR Code will be called a Gatekeeper.

When a Personal QR Code is scanned using the browser-based interface provided by this application, this application will open a signed URL in a browser tab on the Gatekeeper's mobile phone.

The browser page would display a simple visual indicator – such as a green circle -- relating to the COVID-19 status of the bearer of the Personal QR Code.

As previously discussed, Contact Tracing Applications will only allow a request for a Personal QR Code if the on-device Contact Tracing Application shows that its user has tested negative (verified as "no COVID-19"), and/or has not been in proximity with any person who is a known carrier of COVID-19.

Therefore, only qualified Persons should be bearers of valid Personal QR Codes.

Gatekeepers can easily be instructed to look for the signed domain name of this application in their browser URL area after scanning QR codes.

If the scan of a QR code does not display the proper visual indicator, and within the browser-based interface provided by this application, the Gatekeeper can easily reject the bearer.

3. Settings Available to Control Users

Control Users will be able to invite Contact Tracing Applications to integrate with this application. When a Contact Tracing Application registers and integrates with this application, the Contact Tracing Application's integration will be shared within a single deployment of the application.

For example, if single deployment of the application is shared by five Control Users, then the Contact Tracing Applications set up and authorized by each Control User will be shared among the five different Control Users.

However, all of the Control Users may not agree on which Contact Tracing Applications should be trusted. Therefore, each Control User will be able to select which of the available shared Contact Tracing Applications it trusts and wishes to use for its purposes.

For this reason, each Control User will also be able to use this application to generate a separate QR code to control Gatekeeper access. This QR code will be called the "Gatekeeper QR Code".

Gatekeeper QR Codes will be generated by each Control User in the Control User's account in this application. Gatekeeper QR Codes generated by a Control User will only work with the specific Control User's account. In addition, each Control User will be able to share and distribute the Gatekeeper QR Codes created within the Control User's account.

In this way, each Control User will be able to use the "Gatekeeper QR Codes" feature to limit the use of the Contact Tracing Applications it wishes to trust. For example, only the Personal QR Codes from the Contact Tracing Applications that are selected and authorized by the Control User will deliver positive indications. All others will be rejected.

Control Users could also use the Gatekeeper QR Code feature to limit access to this application to only authorized persons.

For example, a Control User that is a governmental entity could authorize only certain types of businesses (such as restaurants, but not night clubs) or facilities (such as public museums, but not private movie theaters) to use the application.

Similarly, a Control User that is a business could limit access only to certain security employees who would need to function as Gatekeepers, such as security personnel at the doors to a factory.

DETAILED USER STORIES:

This Section illustrates how this application will function through hypothetical uses cases.

1. Use Case One

Simon owns a restaurant in New York City. If he doesn't get his business back to normal soon, he will go bankrupt.

However, he wants to make sure his customers don't infect each other with COVID-19, and he also wants to keep his employees safe.

What can Simon do?

He should start using FreeFromCovid.com!

Simon can sign up with FreeFromCovid for free at: https://FreeFromCOVID.com Simon would then become a Control User.

When Simon logs in, he will see a "My QR Codes" tab. A table in this "My QR Codes" tab will be empty, because Simon is a new user, and has not added any "Gatekeeper QR Codes" yet.

Simon will also be able to open a "My CTAs" tab. A table in this "My CTAs" tab will be empty, because Simon is a new user, and has not added any Contact Tracing Apps (CTAs) yet.

He can also open an "Available CTAs" tab. When Simon opens the "Available CTAs" tab, he will see the CTAs that other Control Users have already added. Simon can select from these to use for his own bar.

In this hypothetical, the other Control Users have already added 37 CTAs. Simon selects 5 of the 37 available CTAs in the "Available CTAs" tab. These 5 CTAs will now appear in the table in Simon's "My CTAs" tab.

Simon should now go to his "My QR Codes" tab, and press the "Get New QR Code" button, and provide a name for this "Gateway QR Code".

Simon has waiters, bartenders, and a person at the door of his restaurant to greet customers when they arrive.

Simon can email this "Gateway QR Code" to his employees. He can also print the "Gateway QR Code" on a piece of paper to give to them.

When the employees come to work, the employees should scan this "Gateway QR Code" with the camera on their phone.

When the employee scans the "Gateway QR Code", a browser page will open on the employee's phone displaying certain functionality from our application. This browser page functionality will expire in 8 hours.

Simon's employees can then scan the "Personal QR Codes" on the phones of all of Simon's customers as they come in to his restaurant.

This way, Simon has met his goals.

2. Use Case Two

Martin lives in France. He uses the French contact tracing app (CTA) all the time.

Martin travels to New York City for a conference, and wants to go to Simon's restaurant (see Use Case One). Martin learns that a fraudster created a fake app that looks like the French CTA, but in fact the fake app only shows that every user has no COVID-19 contacts.

How can Martin prove that his app is the real one?

He should start using FreeFromCovid.com!

In this hypothetical, our application is integrated with the French contact tracing app (CTA) that Martin uses.

Martin's French CTA has a "Get QR Code" button in it. Martin can only use this button if his on-phone app shows that he has no contacts with any COVID-19 infected person. If Martin has been tested to have COVID-19, or if he has been too close to a known COVID-19 infected person, the button will be disabled.

Martin presses the "Get QR Code" button in the CTA app on his phone. The CTA app on Martin's phone sends a request for a QR code to the CTA's servers.

Martin's CTA is a "Contact Tracing App" user in our application. The CTA's servers route Martin's request to our application.

Our application authenticates the French CTA's request, and generates a Personal QR Code. Our application inserts the Personal QR Code in a temporary web page accessible through a browser. Our application then returns the browser page address to the French CTA's server.

The French CTA's server then routes the browser page address from our application back to Martin's phone. The web page with the Personal QR Code from our application opens in a browser on Martin's phone.

Because the Personal QR Code from our application appears in the browser page on Martin's phone, Martin can show his Personal QR Code to anyone or to no one.

With Martin's explicit permission and consent, the QR Code can now be scanned by one of Simon's employees at the restaurant in New York City.

Simon's employees already scanned Simon's "Gateway QR Code", and have the browser page from our application open on their phones. They are ready to scan Martin's Personal QR Code using the browser functionality from our application.

Simon selected the French CTA as one of his approved CTAs, and the French CTA appears in the "My CTAs" tab in Simon's account.

When Simon's waiter scans Martin's Personal QR Code, our application sees that it was requested by the French CTA. Our app checks to make sure that Simon authorized the French CTA. Then, our app verifies that Martin's Personal QR Code is still valid.

If so, then our app in the browser on Simon's waiter's phone changes to show a green circle. Simon's waiter understands this means Martin can come in to Simon's restaurant.

The web page from our application shown on Simon's waiter's phone also includes a NEXT button, and a PAUSE button.

Because Martin came to the restaurant with a group of his friends, Simon's waiter presses the NEXT button. Simon's waiter can now scan the Personal QR Codes of more people in Martin's group using our application, and allow them to enter Simon's restaurant.

3. Use Case Three

Martin wants to visit one of the New York Public Library locations while he is in New York City.

The New York City government is checking all people for COVID-19 before they can get into the public library buildings.

However, the New York City government does not want to use our servers to run FreeFromCOVID. Instead, because we offer FreeFromCOVID as open-source app for governments, the New York City government is running our application on their own servers.

How can Martin get into the Mid-Manhattan New York Public Library building?

He can use FreeFromCovid.com!

The New York City government wants to encourage tourism, including from France. The New York City government authorized the French CTA as one of the approved CTAs for various New York City government buildings.

However, the New York City government does not want too many users accessing its account. The New York City government also wants to authorize foreign CTAs only for its facilities that allow public access.

Therefore, the New York City government set up Control User accounts in its installation of our application for each of its facilities, including the Mid-Manhattan New York Public Library building.

The Mid-Manhattan New York Public Library building has its own Control User account in the New York City government's deployment of our application. The Mid-Manhattan New York Public Library building selected the French CTA from the "Available CTAs" table, and the French CTA appears in the "My CTAs" tab in Mid-Manhattan New York Public Library building's account in our application.

Martin presses the "Get QR Code" button in the French CTA app on his phone, and the CTA app on Martin's phone sends a request for a QR code to the French CTA's servers.

The French CTA's servers then route the request to all installations of our application that have connected with the French CTA.

The French CTA will know how to contact the New York City government's installation, because the New York City government had to invite the French CTA to connect with the New

York City government's installation, and the French CTA would have an account on the New York City government's installation.

All the installations of our application that have connected with the French CTA will generate a Personal QR Code using the same confidential and secure encryption methodology. Each such installation of our application returns the address for a browser page displaying its generated Personal QR Code back to the French CTA's server. The French CTA accepts and uses the first response it receives, and ignores the others.

In this case, a Personal QR Code from another installation -- perhaps one in Paris -- reaches the French CTA's servers first. The French CTA routes the Personal QR Code from the Paris installation to Martin's phone, and ignores the others.

Martin's phone now displays the Personal QR Code from the Paris installation of our application.

The Paris installation generated its Personal QR Code using the same confidential and secure encryption methodology that all the other installations of our application used. Therefore, the Personal QR Code from the Paris installation can be decrypted by any other installation of our application, including the New York City government's installation.

The guard at the Mid-Manhattan New York Public Library building scanned the Mid-Manhattan New York Public Library building's "Gatekeeper QR Code" on her phone. Our application is still open in a browser page on the phone on her app.

The guard uses our application in the browser page on her phone to scan the Personal QR Code on Martin's phone. The New York City government's installation uses the confidential and secure encryption methodology to determine that the request came from the French CTA.

The New York City government's installation of our application checks to make sure that the Mid-Manhattan New York Public Library building authorized the French CTA.

Then, New York City government's installation of our application verifies that Martin's Personal QR Code is still valid.

If so, then our application in the browser on the guard's phone at the Mid-Manhattan New York Public Library building changes to show a green circle.

The guard understands this means Martin can come in. She lets Martin in, confident that he is free from COVID-19.

The web page from our application shown on the guard's phone at the Mid-Manhattan New York Public Library building also includes a NEXT button, and a PAUSE button.

Because Martin came to the building alone, and no other tourists came there at the same time, the guard presses the PAUSE button.

When the guard presses the PAUSE button, our application in the browser on her phone changes back to the original view, and turns off the camera on her phone to save power.

