Prior Location Provenance ("Safe14")

UK Patent Pending # GB2003702.4

1. Given the COVID-19 pandemic, it is critical to be able to identify traveler's locations within the prior 14-days. Travel restrictions are being imposed, but they are hard to enforce except on an economically destructive blanket basis, as travelers can use a third-party waypoint to obfuscate prior locations. How can officials be assured of travelers' movements to avoid a blanket ban? And what can individuals do to reassure them? And how can this be done in a way that doesn't create a centralized database of personal information that becomes an unacceptable privacy intrusion and a honeypot for data leaks and hacks?

2. Each traveler registers using an Android or iOS phone via a through the browser application (or by downloading a native application) that takes a picture of the subject's face and irreversibly converts it on device to a unique hash (EgHash™) and generates a QR code containing that EgHash which is stored on the device used. *(insert the explanation of hashing / hash matching and reference prior US filing(s) claiming priority is applicable)*

3. Optionally, the QR Code could be sent to the traveler by email or SMS in order that they have it available on other devices. The QR Code can also be printed for availability off-device.

4. The EgHash and QR code contain no personally identifiable information (PII) simply the irreversibly transformed biometric-originated data that enables probabilistic comparison to later-generated EgHash.

5. The sole utility is that the EgHash can be compared to any other EgHash by proprietary AI *(insert the explanation of hashing / hash matching and reference prior US filing(s) claiming priority is applicable)* and the probability of both relating to the same person predicted. At registration, the EgHash is checked against prior hashes to make sure that it is unique. One face can only have one hash.

6. The EgHash is stored in a database with date/time, and encrypted latitude/longitude and the QR Code is stored on-device.

Install App - Take Selfie - Click "Check In"

7. At each point along a journey (e.g. flight boarding) a traveler presents their QR code which is scanned, and their facial biometrics hashed and compared to the EgHash in the database. The database is updated to record the location (via a geolocation API) and date/time that the QR code was scanned. The QR code is used to make the matching process 1-1 vs. 1-n for speed and accuracy.

8. Officials with a security key to either use a dedicated application or access a sever based application can verify the QR code against the subject's facial biometrics and query if the QR code has been seen in an exposed area. If the answer is yes, the official may ask follow-up questions and determine if quarantine is required, imposing if needed.

9. The database will only respond to a "zero-knowledge-proof" interrogation such as "has this QR code been seen in a designated area in the last 14 days?" and will provide only a yes/no answer.

Traveler Presents QR Code – Official Snaps Code + Photo of Traveler - App Displays Pass or Fail

10. A complimentary approach is to verify that the QR code has consistently been logged in safe areas for a rolling 14 days. Under this approach, the user self-registers and the application records the device location prompting Facebook-style "check-in" with facial biometric verification at random times. Failure to verify resets the 14-day clock. T

11. The process could be undertaken in advance of travel but also used as a means of monitoring quarantine. Quarantined travelers are registered by the relevant official on their official device and the URL for log-in and traveler's QR code sent to the Traveler by SMS. In this case, the database stores the location of quarantine, the number of days and the case # and email address for automatic notification of check-in failures. The database could also provide a direct (permissioned) link to a database that stores PII and other data relevant to monitoring and enforcement. If a check-in fails, the traveler and a relevant official are notified of the failure.

Traveler Clicks on "Check-In" - Takes Selfie – Done

12. The database can be server or blockchain based. Ideally, there is multilateral adoption, but a single jurisdiction or a commercial entity may unilaterally impose usage as a condition of entry/passage/use. In the case of multiple separate implementations, in due course, there could be a federated implementation. The location database would be expunged periodically (e.g. every 21-days).