Analysis of DP-3T by considering 6 strategies of DPbD

1. Minimize Collection:

The DP-3T only use the random messages sending to users and the messages phones “heard” from nearby phones. So, it does not use GPS which protect the location of users and without acquiring for users’ personal information.

1. Minimize Disclosure:

The only information the app may collect is the random gibberish send to one’s phone and the random strings it “heard” from other phones[1]. There is not any sensitive personal information, no worries for disclosing it.

1. Minimize Linkability:  
     
   The DP-3T protocol works off the basis of Ephemeral IDs(EphID)[2], that is to say, the application can link nothing to the EphID. In this case, each personal device verifies contact logs locally and contact logs are never linked with third party.
2. Minimize Centralization:  
     
   From start to the end, the contact log will only be verified locally(on the application itself) but never reach to the server.
3. Minimize Replication:  
     
   In the whole process, the only data user might be replicated is the EphID, but firstly it is temporary but not the true identification; secondly, every user’s EphID should be unique, it does not meet the possibility to be replicated.
4. Minimize Retention:  
     
   The data will be kept for a short period in this protocol(especially when people being detected as infected), but it will be refreshed and updated from time to time after this guy’s recovery. In the end, data exists all the time but nothing remains in the database forever.

Reference:

1. [PROTECTING LIVES & LIBERTY (how contact tracing apps can foil both COVID-19 and Big Brother)(PDF).GitHub. Retrieved 26-04-2020](https://github.com/DP-3T/documents/blob/master/public_engagement/cartoon/en/comic-en.pdf)
2. [Decentralized Privacy-Preserving Proximity Tracing. Wikipedia](https://en.wikipedia.org/wiki/Decentralized_Privacy-Preserving_Proximity_Tracing)