Exposure Tracking DP: DPP Questions and Answers. Also FAQ, v0.
March 18, 2021
Also note that shorter versions of some of these answers are also available on piazza.

1. **Testing**: There were a number of questions in this area. First, an update (also noted on piazza) is that testing occurs for each person every other day on a continuous basis. Consider an example. A person is tested on day N at noon. If the test is positive, it is assumed that they were infectious as far back as noon on day N-1. Furthermore, it may take some time to analyze the test. The latest a positive test result will be made available is day N+1 at noon. So, figuring out who was exposed will require a bit of working backwards. Exactly how that is done is part of your challenge. Second, another part of this set of question was about getting test results into the exposure tracing system. Tests are administered by a health care system. As you will have noticed, in the example systems, in the first two, the health care system reports test result directly into the exposure tracing system. In the third, positive test results are only available in the exposure system if the person in question chooses to make that information available. The point is that exactly how and by whom the positive test result information gets into the exposure tracing system is a design choice that you will need to make and justify.
2. **Presence and use of the app**: For purposes of your design, we are assuming that every person associated with the university has a smart phone, the app is installed, it is running at all times, and the radios are always turned on. Of course, this is an ideal situation, and if we have time, we may relax that later. But for the present, assume the app is always running and all phones keep themselves and their radios turned on at all times.
3. **Measuring "contact":** Again, we have idealized the situation. We are assuming that no transmission of BLE occurs between people with a "contact" barrier between them. This might include walls, glass or plexiglass partitions, etc. Contact can only occur between people without a barrier between them. That said, in our simplified situation, the signal strength of any received BLE signal provides the basis for evaluating distance apart. The system will do that for you. For any received signal, the system can map directly between signal strength and distance apart. Again, in looking at the three example apps, one of them does not simply reject any reading of more than the basic distance away, but also factors in period of contact, so a longer contact at a greater distance is equivalent to a shorter contact at a closer distance. It is not necessary that you take an approach such as this, but it is an option. If you choose an adaptable scheme you will need to explain and justify it.
4. **Privacy**: Metrics for privacy are few and far between. You are not expected to measure privacy, but that said there are other ways to evaluate whether an approach provides more or less privacy, of what sort (what are the privacy risks), and whether the user has any choice or control over their privacy settings (which contrasts with what options the underlying system gives them). Although these are all issues to consider in your design, remember that you are not designing a UI here. You will want to decide on the balance between user privacy and other functions and design to fit the balance you believe is right. Although it is not necessary, if you want to give the users a choice about privacy, you will need to design your system to handle all options. Although you are not designing a UI in this project, you might want to consider the effectiveness of giving users a set of choices. If they have choices, will they understand the implications of those choices? If they make a choice that is contradictory to what they wanted and thought they were getting, what could go wrong with this? What impact will their choices have on your ability to support the functionality of the system that you want to achieve? How much complexity will this add to your overall system?

5. **Security**: As the spec is written, there is no consideration of security. That means that the spec writer assumed that all users are not malicious and that they are not concerned with intruders.
6. **Power utilization**: The spec does not provide numbers for power utilization, but there are several observations to make without numbers. First, BLE is very low energy. It uses extremely little power. You can assume that it is on all the time and that each phone even if more or less asleep is sending and receiving at all times. As noted in #2, you can assume that all phones are "running" all the time, so they can do simple things like sending, receiving and logging the BLE signals all the time. Second, in contrast, WiFI radios require relatively a great deal of power, especially for sending and receiving, as opposed to listening. Your usage of WiFi is under your control, so you will want to think about and design for efficient use of WiFi. Third, complex computations will certainly take more energy, so something that does something like $O(N^2)$ computations where N is large is probably not something you want to do on the phone or at least not very often. In the current version of the spec, power utilization is not considered numerically, so the best you can do is either estimation or qualitative evaluation of power utilization.
7. **Fault tolerance**: For the present we are assuming no failures. A good design would be adaptable a variety of failures including the central server, the phones, the routers and the networking elements (e.g. links) failing, but as the spec is written, failures are not considered.
8. **Data formats, communication and storage**: This covers several issues. First, consider what is on the phone. The spec tells you approximately what is stored for each BLE message, if you choose to use the default. If you find that there are ways to organize the data more efficiently, or aggregate or compress that data, you may choose to do that, but you will need to explain what you are doing and at what cost (e.g. loss of detail or additional computation, etc.). The storage utilization of this set of data is discussed in the spec. If you need to store other information on the phones, you will need to design that, explaining what it is, how it will be organized, and how much storage it will require. The only other part of the "data" story that is provided to you is the set of databases that provide all the infrastructure about the university, on the central server. You do not need to be concerned with either how much storage they require or how they are organized. This includes who lives where, who is involved in which courses, etc. You will need to be concerned with which of the data related to both contact and exposure is stored where and how that will be organized. Also, if you use the logging information from the routers, you will need to figure out where that is needed, how it is stored, etc. In terms of communicating data, you will need to determine which data needs to be moved where and when. You may find that you need to define specific protocols to do this well, within the constraints of your design. If you do not need to define a new protocol, then an explanation of which existing protocol will be used and under what circumstances will be needed, with a justification for your choices either way.