COVID-19 contact tracing: 8 privacy questions explored - a reply to de Montjoye et al.

Henry Price and Hugh Lawson-Tancred

22 April 2020

The privacy examination in the paper is structured around three "toy" protocols for the design of an app which can maximise the utility of contact tracing information while minimising the more general risk to privacy. On this basis, the paper proceeds to introduce eight questions against which they should be assessed. The questions raised and the protocols proposed effectively amount to the creation of a game with different categories of players able to make different moves. It is therefore possible to analyse the model in terms of optimal game design.

***

The overall purpose of the game is to maximise (pure) contact information while at the same time minimising (noncontact) personal information. As a typical user, Alice should know that she has been in contact with somebody (in fact Bob) without knowing that her contact is indeed Bob or indeed knowing anything else at all about Bob. Her ignorance of the latter two facts is as important on privacy grounds as her knowledge of the first on grounds of safety.

Contact information, however, can connect with personal information in two ways. The first way is that (i) personal information is needed to establish contact information, and the second is that (ii) personal information can relatively easily be derived from contact information. The ideally designed game will enable the exchange of contact information without such information having to be established on the basis of any more general personal information or being the possible source of a derivation of such more general personal information. Contact tracing should not involve any sharing with either other users or the authority of trajectory/social graph information (from which identification is possible either by the authority or by the adversary).

Given these overall parameters, it seems possible that both the protocols and the questions/answers in the paper could be advantageously altered.

***

Firstly, in terms of the categories of player, the authority and the adversary seemed to be relatively straightforward (though the details could perhaps be

fleshed out if any specific app were to be considered/assessed). However, the user category of player could perhaps be supplemented with a subdivision of the non-infected group into *at risk* and *risk-free*. Presumably non-infected users who have been in contact with a (previously non-infected) user who has become at risk will themselves become indirectly or secondarily at risk, and this change of their status might be worth notifying either to them or to the authority (in the interests of tracking the contagious spread).

***

Secondly and more importantly, there is considerable scope for changing the proposed protocols in order to enable optimisation of the data flow objectives.

On this basis, the first protocol needs to be amended so that the authority does not reveal the entire trajectory of an infected user to all non-infected users. To avoid such undesirable disclosure, the authority has to know the trajectories of all users, whether infected or not. This arrangement, by which all information is accumulated with the authority and the minimum possible disclosed to users, could be protocol 1a. It seems to be a limitation of trajectory-based apps (and therefore a reason for preferring identifier-based apps) that with them it is not possible to avoid disclosure of entire trajectories to either other users or the authority (or both). A decision therefore has to be taken, on this paragraph, between dispersion and aggregation of information.

This is presumably at least part of the motivation for considering identifier-based protocols; however the differences between the second and third protocols could also be clarified further. There are two such differences. The first is that protocol 2 has a fixed identifier, whereas protocol 3 has a variable identifier (to use a suboptimal term). This is the more conspicuous difference, and it plays a larger part in the response to the questions. The second difference, however, is that protocol 2 also sends its full history of identifier encounters to the authority, whereas article 3 only sends its identifier change record. In the case of protocol 3, the authority is not able to figure out for itself the now at risk users. So it sends the variable identifiers whose status has changed to infect. This seems to decrease the privacy of the infected users while increasing that of the non-infected users (both at risk and risk-free). This difference also seems to have a material effect on the privacy vulnerability. For example, does it reduce or increase the knowledge of the authority about trajectories/social graphs of either group? If the authority is able to connect the varying identifiers, then it acquires a finer grained level information about the relevant users. Protocol 3 is, therefore, in effect a bet on the inability of the authority to spot the continuities in series of variable identifiers.

There seems to be a further assumption built into protocol 3. Any information available either to the authority or to any or all users is in principle also potentially available to the adversary. The existing game model thus makes the further assumption that identifier information on mobile phones is more open to hacking than trajectory information. However, such an assumption is not immune to challenge. It needs to be clarified what are the relative strengths and weaknesses of the protocols with respect to the adversary.

***

Thirdly, the answers to the specific questions also need to be reviewed (partly in the light of the queries about the protocols). We now look in turn at some of the ways in which the answers to the 8 questions could be changed.

Question 1. Protocol 1 obviously discloses the whole trajectory of infected users to the authority. The disclosure also to non-infected users can be avoided, but only at the cost of non-infected users also revealing their entire trajectories to the authority. This would be the move from protocol 1 to protocol 1a. If there is perceived to be an inverse connection between threat status and privacy entitlement, then it would seem that this change of trajectory-based protocol would be unfair. A larger number of users who do not constitute a threat would see their privacy eroded in order to protect the privacy of the smaller number who have become infected. (It should be noted that this objection applies irrespective of whether or not any form of blame is to be attributed to the change to infected status (e.g. by disregarding social distancing etc).)

In terms of the identifier-based protocols, the improvement provided by protocol 3 over protocol 2 depends on the authority not being able to reconstruct the pseudonymous social graph across the changes of identifier. As discussed in connection with the protocols, however, it is not obvious that it will not be possible for the authority to do that.

Question 2. The same objection to the greater innocuousness of protocol 3 over protocol 1 and protocol 2 arises as with question 1. Presumably if the game is to rely on "special measures" to "limit the risk", then those special measures should be applied at the level of the authority not the users (where they can more easily be circumvented and less easily monitored). It could also be argued that reidentification by either the authority or other users automatically raises the risk of reidentification by the adversary.

Question 3. Protocol 1 does indeed give the right answer on this question, but only at the cost of giving too much information to non-infected users. Again the difference between protocol 2 and protocol 3 is not clear. It is a reasonable supposition that the identities of the infected group are more sensitive than those of the non-infected. The former are (presumably) less numerous, but they are more vulnerable to potential stigmatisation/vigilantism. If that assumption is right, it would form a strong objection to protocol 1. What this suggests is that a more nuanced distinction needs to be drawn between the type of threat posed by the authority and that posed by other users.

Question 4. Protocol 1 obviously fails this test in its existing form, but that can be prevented by letting the authority know the trajectories of non-infected users (protocol 1a again). Protocol 3 seems to be definitely worse than protocol 2 on this question, however it is tweaked. This reinforces the suspicion that protocol 3 is not preferable to protocol 2 in any respect. Given the presumably greater practical difficulty of deploying protocol 3, this would seem to be a very solid grounds for rejection of protocol 3 in general.

Question 5. This seems to be the crucial question for the overall objective of the game as outlined at the start. It is not obvious how the protocols can be

structured to enable either users or the authority to gain only and exclusively specific contact information without either supporting it with more general personal information or creating a situation in which wider personal information can be triangulated from the contact information. This highlights exactly what any privacy-secure contact tracing must achieve: the Holy Grail is pure contact information, uncontaminated by any noncontact personal information.

Question 6. This seems to raise again the question whether concentrating information with users or with the authority constitutes the greater security risk. Most recent major hacks have focused on concentrations of data, suggesting the more disaggregation the better. Hacks from large numbers of dispersed users have been less effective, so far as can be known.

Question 7. It is not clear what additional protections could be made available. One possibility would be some kind of time limitation of the information or preventions on its further disclosure. Presumably this would in practice be a question about encryption rather than game design. The other obvious way to develop such protections would be through legal/regulatory constraints, but they would also clearly fall outside the scope of the intrinsic app-modelling game under consideration.

Question 8. As in many other areas of data protection, the may be a trade-off between the transparency of the system and its privacy-protection and/or security. It may not be possible simultaneously to optimise all three parameters. On the other hand, a possible way of at least partially squaring this circle is that some form of blockchain might be deployed here.

***

This (perhaps modified) game design approach seems to offer a good basis for a design intended to optimise the protection of the relevant moral assets. Non-infected users have an interest in learning about vulnerability-increasing contacts, but have no right to any other information about infected users. Infected users have a duty to maximise knowledge about their contacts, but the right not to have any further information about them disclosed. (As we have seen, the right of the infected might outweigh that of the non-infected on the grounds of the risk of vigilantism, whereas it might also be thought to be outweighed because of the possible culpability of infection given the level of public knowledge. This is clearly a value, not a pure design, issue.) The authority has the right (and possibly duty) to be as informed as possible about the pattern of spread of the epidemic, but it should be prevented from acquiring (and indeed retaining) any more than the essential information about the users under its jurisdiction. The adversary has no rights in this context and is simply a threat to be minimised.

The most significant improvement to the approach proposed, in our opinion, would be to replace protocol 1 with our protocol 1a. We are agnostic as to the general preference for trajectory/identifier approaches, but we suspect that with the latter protocol 3 on balance creates a greater privacy risk than protocol 2.

***

Background reading

1. Ada Lovelace Institute (2020). Exit through the App Store? Ada Lovelace Institute publications.

2. De Montjoye YA, Hidalgo CA, Verleysen M, Blondel VD. Unique in the crowd: The privacy bounds of human mobility. Scientific reports. 2013 Mar 25;3:1376.

3. Ferretti, L., Wymant, C., Kendall, M., Zhao, L., Nurtay, A., Bonsall, D.G. and Fraser, C., 2020. Quantifying dynamics of SARS-CoV-2 transmission suggests that epidemic control and avoidance is feasible through instantaneous digital contact tracing. medRxiv.

4. Google-Apple (2020). Contact Tracing: Cryptography Specification, April 2020

5. Privacy International (2020), 'Bluetooth tracking and COVID-19: A tech primer', Privacy International, March 31

6. PEPP-PT (2020). Pan-European Privacy Protecting Proximity Tracing: Context and Mission, PEPP-PT manifesto

7. Radaelli, L., Sapiezynski, P., Houssiau, F., Shmueli, E. and de Montjoye, Y.A., 2018. Quantifying surveillance in the networked age: Node-based intrusions and group privacy. arXiv preprint arXiv:1803.09007.

8. Raskar, R., Schunemann, I., Barbar, R., Vilcans, K., Gray, J., Vepakomma, P., Kapa, S., Nuzzo, A., Gupta, R., Berke, A. and Greenwood, D., 2020. Apps gone rogue: Maintaining personal privacy in an epidemic. arXiv preprint arXiv:2003.08567.

9. M. Scott, L. Cerulus and L. Kayali (2020), 'Commission tells carriers to hand over mobile data in coronavirus fight', Politico, March 23

10. Sharad, K. and Danezis, G., 2014, November. An automated social graph de-anonymization technique. In Proceedings of the 13th Workshop on Privacy in the Electronic Society (pp. 47-58).

11. M. Sweney and A. Hern (2020), 'Phone location data could be used to help UK coronavirus effort', The Guardian, March 19

12. Troncoso, C. et al (2020). Decentralized Privacy-Preserving Proximity Tracing, Github DP-3T documents, 12 April 2020