Submission to the Special Committee on COVID-19 Response on the topic of Covid-19 Testing and Contact Tracing

Dr. Stephen Farrell and Prof. Doug Leith
16th June 2020

We would like to thank the committee for the opportunity to make our submission on this topic. This is a joint submission by Prof. Doug Leith and Dr. Stephen Farrell, of the School of Computer Science and Statistics, Trinity College Dublin. Our submission relates only to technology issues with the planned HSE contact tracing "App" and to such Apps in general. Our expertise is in computer systems, security, privacy and networking and not in epidemiology. This submission reflects our personal views and not those of Trinity College Dublin.

We have carried out independent analysis and tests of the technologies underlying COVID-19 contact tracing Apps, initially based on the open-source version of the Singapore "OpenTrace" App, and more recently based on the Google/Apple Exposure Notification (GAEN) system that will be used by the HSE App. We have not, at the time of writing, seen or done tests with the HSE's own App. We have published a number of results from this work at https://down.dsg.cs.tcd.ie/tact and have additional results we plan to publish in upcoming days. Our publications on this topic have not so far been peer-reviewed as we felt it important to make them available in a timely manner for the technical community including the developers of Apps such as the HSE's.

We believe everyone with whom we have interacted on this topic has the best interests of Irish and other citizens at heart. That includes Civil society organisations, the HSE and their contractors, Google and Apple employees, and individual Irish-based and international experts and developers. We were assisted in gaining the authorisation required from Google and Apple to test the GAEN system thanks to HSE staff. Trinity College Dublin provided funds for us to acquire the handsets we used in testing.

Results and Recommendations

Our tests so far indicate that it will be challenging for any such App to be effective. For example a train carriage or bus provides a very difficult environment for such Apps, and how a person carries their phone has a major impact, but is impossible to control.

The highest-level take-away is: **the HSE App might not be effective, but is worth trying, if, but only if, that attempt is made in the knowledge that it is an experiment that may not succeed**. Messaging to the public should reflect that likelihood. How to do such messaging is not within our area of expertise.

At one level down:

- If COVID-19 tracing Apps could materially improve contact tracing that would be beneficial. That requires that those Apps materially improve the overall contact tracing and testing system, so what will count is the added value of the App to that overall system. It is not clear at present if Apps will or will not provide such an improvement. When deploying a contact tracing app measures should therefore be put in place to collect data on the added value of the app within the larger contact tracing and testing system. Such measures will likely be as an addition to the interactions between contact tracing personnel and the public and not as a technical feature of the HSE App.
- It remains worthwhile expending effort to experiment with such Apps in Ireland, but that must be done with an awareness that there is a high probability the results will be negative or inconclusive. In other words - do keep trying, but do not depend on (or claim) inevitable success - inconclusive results or failure seem to us more likely at this point. There are also security and privacy risks inevitable when deploying these Apps, so there is also a need to ensure proportionality considering both the costs and benefits.

There are two high-level risks that may cause such Apps to be ineffective:

- Bluetooth Low-Energy (BLE) may not determine proximity with sufficient accuracy due to the vagaries of radio propagation in real-world environments and with how devices are carried. If so, that will be due to the laws of physics and not the failings of developers or those promoting the use of such Apps. As BLE proximity is complex and varies by handset, Google and Apple probably need to be part of the development of any credible solution, if a working solution exists, which is uncertain.
- Insufficient use. That can be caused in a variety of ways - in a fast changing environment, one cause for this risk is a lack of trust in various of the entities involved, including government, Google and Apple and the potential for future abuses of this technology for commercial purposes. In our opinion, people are justified being suspicious of Google and Apple when it comes to tracking, as mobile Apps of many kinds are widely known to track people pervasively. Awareness campaigns may thus be unable to address this risk. (We nonetheless believe Google and Apple are acting in good faith in this effort - such mistrust is just one of the costs of surveillance capitalism.)

We would also like to draw attention to some other aspects of such Apps that may not feature in other submissions:

- Further entrenching of the Google/Apple duopoly via socially-important functionality such as this is undesirable. A short-term emergency may make that acceptable, if it is clear that the emergency will be mitigated by the Apps. Today, that is not clear.
- If these Apps are deployed at scale, it is critical to devote as much effort and attention to undeployment at the end of the emergency, perhaps via legislation, so that the infrastructure is not re-purposed for commercial, or other, surveillance.
- Deploying such Apps may encourage others (employers, transport operators, stores) to require use of similar technologies, without the benefit of the kind of scrutiny being provided by this committee or by technologists worldwide. That could

badly infringe on various rights and freedoms. The HSE App is not the only relevant thing that could have security or privacy implications in this space, but the HSE App may set a local precedent that could be widely followed. Society might benefit if the committee revisit that topic as such systems are deployed by private entities in the coming months.

- It is good that the HSE have promised to publish their code. That is necessary and the sooner the better. The HSE should also publish the code used in their various backend systems and not only the code that runs on the mobile handset.
- The same is not so far true of the implementation of the Google/Apple systems which are a part of their mobile operating systems and remains closed source and with limited documentation. We would encourage the committee to request Google and Apple to open-source their implementations as well. Without that, Irish citizens will be vulnerable to potential errors made by Google or Apple developers.
- We have seen updates of the Google implementation pushed out while we tested. That is quite understandable, but shows Google or Apple could at any time affect the false positive/false negative rates of the HSE App with no control or oversight by the HSE, Irish government or the technology community.

Bluetooth Low Energy Proximity

Based on the tests we have conducted so far, we believe the first risk of inaccuracy in distance estimation is very significant. While accuracy can be demonstrated in tests in some laboratory conditions, our tests so far in more real-world scenarios [1] indicate that accuracy in a real deployment will be far more challenging. Follow-up work has continued to indicate that these challenges are real and hard to handle, for example the relative orientation of two devices (whether they are both top-up, or front-to-front) has a significant effect on the signal strength seen. Additionally, we have seen significant and large variations in received signal strengths when different models of device are tested under the exact same conditions. (We plan to publish these results shortly after this submission is due.)

To explain the BLE proximity issue in more detail: BLE is a radio technology used in mobile handsets, for example, to connect handsets to headphones. BLE is intended for use with nearby devices, and so uses low power radio transmission. As radio waves propagate roughly spherically in all directions, the power of the transmission weakens over distance, as do the ripples or waves caused by a stone dropped into water. If you start by making a set of measurements with different sized stones and different distances and if you know the size of the stone and the size of the wave when it reaches you, you can estimate how far you might be from where the stone entered the water. However, if you do that in a bath, waves will bounce off the sides and make your estimation much less accurate. Or, if there is a body in the bath, that will affect your accuracy too. While no analogy is perfect, the same effects happen with BLE radio distance estimation - a phone upside down in a back pocket when sitting on a metal chair will be estimated to be much further away than one nicely oriented in a shirt pocket. One result is that a person 4 metres away in a train carriage can appear "closer" than one 2 metres away due to reflection of the radio waves off the metal carriage walls, floor and ceiling. It is unclear if even the engineers of Google and Apple and the HSE can cater for all these possibilities without generating many false negatives (where someone truly in proximity is missed) while keeping an acceptable level of false positives (where someone is mistakenly considered as having been in proximity).

For COVID-19 tracing Apps, the effect of a false negative is that someone who may be infected goes undetected and infects others. The effect of a false positive may be that someone needlessly isolates for two weeks.

Privacy and Security

The typical tools used by App developers for commercial Apps often include features to allow developers track how their Apps are being used. This can be, and often is, done in a manner that is extremely privacy invasive. For example, such that every time a person opens the App on their phone, that information is sent to a server located in some other country, typically in the United States or under the control of a company based there. We carried out an analysis of the Singapore App [2] that indicates that it suffers from such deficiencies. Open-sourcing the HSE App and associated back-end system will enable us and others to ensure that the HSE have done a good job in this respect. We do believe that is their intention but it is in fact easy to make mistakes in this respect and accidentally include trackers via relatively low-level use of libraries and other systems that are part of the commercial mobile App ecosystem.

Various well-known attacks exist against any of these systems, and using estimated Irish numbers, we have documented one method of attack [3] that could lead to approximately four false positives for every real positive whilst a COVID testing station was under attack. We consider the risk that someone attempts such an attack somewhere in the world is high. Once demonstrated, copy-cat attacks in other places such as Ireland would be likely and could damage confidence in the App sufficient to fatally affect utility. Preventing all such attacks is extremely hard and we are not aware of any proposal in this space that has no such vulnerability.

The underlying cause is the need for everyone's handset to accept broadcasts from anyone's handset without real-time strong authentication. This makes the problem roughly as hard as eradicating spam in email. Any system (centralised or not) that fully addressed these threats via strong authentication could require the equivalent of a major overhaul of the worldwide mobile ecosystem, which will not happen in the relevant time-frame.

Undeployment

Planned "undeployment" is an unusual thing for computer applications. As such, it will require additional analysis that we imagine is likely not a part of typical HSE or other development processes, especially when done under time-pressure as is the case here. As one example, the use of new Domain Name System (DNS) sub-domains for server names and the use of new code-signing certificates that can be revoked later may make undeployment easier, more thorough and more convincing, but only if plans are made for that now, before any real deployment. We understand that the HSE may have such plans in place, and those ought be published as soon as possible, even if in draft form.

Summary

We believe continued work on the HSE App is warranted, but all involved need to assume that a lack of demonstrated utility for contact tracing Apps is more likely than success. Do the work, roll it out, but without making unwarranted claims that the overall system will work, until that is in fact demonstrated by experience. Always be ready to stop and take the App down from the App stores. And regardless of success or failure, make sure to ensure that all the infrastructure is dismantled as soon as possible.

References

[1] D. Leith and S. Farrell, "Coronavirus Contact Tracing App Privacy: WhatData Is Shared By The Singapore OpenTrace App?", 2020-04-28
Available: https://www.scss.tcd.ie/Doug.Leith/pubs/opentrace_privacy.pdf

[2] D. Leith and S. Farrell, Coronavirus Contact Tracing: Evaluating ThePotential Of Using Bluetooth Received SignalStrength For Proximity Detection, 2020-05-06
Available: https://www.scss.tcd.ie/Doug.Leith/pubs/bluetooth_rssi_study.pdf
(And attached below.)

[3] S. Farrell and D. Leith, A Coronavirus Contact Tracing App Replay Attack with Estimated Amplification Factors, 2020-05-19
Available: https://down.dsg.cs.tcd.ie/tact/replay.pdf