Boris' Perpetual Tracking Machine (31 March 2020 v1.1)

Having 50% of the population install an app is not an unreasonable expectation, if it is the main item in the daily press conference headed by the Prime Minister, and consequently receives *consistent, accurate, positive media* coverage. We examine here what the app will actually do.

According to an NHSX presentation, shown under a UPD logo, drawing on slides from an Oxford University paper[1], the NHSX 'tracking app' tracks and stores the permanent, unchangeable, Bluetooth machine address embedded in each mobile phone, smart watch, wireless headphones, tablet, or laptop. While measuring social distancing may be a temporary requirement, these identifiers persist in tracking the owner for the lifetime of the physical device. That they are being used is an implementation *choice* by the team building the app.

That a cloud services company has been involved means a deliberate decision has been taken to do excessive work in 'the cloud' – allowing individuals to be tracked, in perpetuity, in ways that should never have been made possible at all.

To be absolutely clear, instead of taking an equally viable approach which would use completely random temporary identifiers broadcast by the phone, permanent trackable identifiers are the *choice* the Oxford University-led team has decided to make.

The 'notify all devices which have been in contact' approach requires the app servers to link a Bluetooth device to an app, and to have a social graph of everyone who sees everyone. Again, this is an implementation choice – were the identifiers random, all infected identifiers could actually be *published* as they wouldn't connect to anything.

Any information that is available to any app will be republished by interested others monitoring the feeds – there is simply too much widespread interest in the level of reporting and the number of those potentially infected to mitigate such impacts.

Many shops already do Bluetooth device scanning, and will have access to those same APIs that NHSX offers the app. To protect its users from the WiFi form of such scanning, Apple already randomises the WiFi MAC addresses of its devices, due to widespread persistent abuse for marketing purposes. At some point after the pandemic is over, Apple (and others) will have to do the same for Bluetooth as well, because of the behaviour that NHSX will be incentivising – seemingly with CDEI's endorsement.

Companies which have already attempted to evade the rules will simply add a sign on their door: "No police, no NHS, no infectees" – with the latter enforced by Bluetooth scanning and an immediate ping to the NHSX servers to check whether each device on its threshold is believed infected. Indeed, such a feature could likely be rolled out immediately by a large number of supermarkets, department stores and shopping malls, given the surveillance infrastructure they have already deployed.

[1] e.g. Figure 1, https://github.com/BDI-pathogens/covid-19_instant_tracing/blob/master/Policy%20forum%20-%20COVID-19%20containment%20by%20herd%20protection.pdf

By their own admission, in the documents we have seen, the tracing app developers have chosen to make technical decisions which increase the social risk of rejection of their approach, because it makes their app easier to build. This is a fundamental mistake.

What does acceptable look like?

1) The app should broadcast a BluetoothLE beacon of a *randomly generated* UUID, which changes every 24 hours or so – and it is those UUIDs alone that should be stored by each instance of the app / processed by the app server.

2) When someone presses the "I have symptoms" button, the UUIDs that have been 'broadcast' in a recent enough time period by the app on that individual's device should be sent to NHSX, and then published. Each instance of the app on everyone's device can regularly pull down that full list of 'symptomatic UUIDs', and see whether any of the randomly generated UUIDs that it has broadcast is included in the current risk list – and then use local information to determine whether that is notifiable to the user. (Subject to a proper cryptographic audit, the results of sha512(UUID of device + UUID seen) could be sent to NHSX, to mitigate some reidentification attacks)

As an aside, the 'user journey' slides shared in the NGO call are fundamentally disconnected from both NHS guidance and the technical implementation; including how the app uses Bluetooth when Bluetooth is turned off. We shall cover further issues in our forthcoming blog post.

medConfidential would of course be willing to input into a meaningful "ethical oversight" process for this app or related initiatives – as we did, for example, in the care.data Advisory Group (CDAG) and across other aspects of Government policy. As with almost everything run by CDEI, however, they haven't been in touch about what it is they are doing; while normally this wouldn't matter, such choices in the current context may have a measurable body count.

medConfidential
31 March 2020
coordinator@medConfidential.org