CASTLEBRIDGE

Changing how people think about information

Data-Driven/App-enabled Pandemic Responses: Data Protection Issues, Risks, and Recommendations

Version Control

Version	Date	Changed By	Comment
2.5	2020/04/26	Daragh O Brien	Extracted from full Report

Contents

Acknowledgements

As with the first edition of this report, we acknowledge the early input of independent experts such as Phil Booth in MedConfidential, Pat Walshe of Privacy Matters, and others.

In this edition, I would like to acknowledge the various academics and researchers who have contributed to the rapid evolution and development of frameworks in this space, in particular for contact tracing. I would especially like to commend those consortia who have adopted a high level of transparency in their publication of materials and their response to questions and their willingness to discuss pros and cons of their proposed approaches and alternative technologies.

I would also like to thank Digital Rights Ireland for their insights on some topics.

Caveats

This extract summarises a report that represents a 'best efforts' analysis of the current state of the nation as of the 22nd April 2020 when the desk research activity was concluded. Some additional minor changes were made based on information that became available on 26th April 2020.

It does not constitute legal advice and it will, by reason of the rapid evolution of the debate and research in these areas in response to Covid-19, contain errors, omissions, and gaps.

Where these are highlighted to us, every effort will be made to update and correct the analysis in a later edition of this report.

Furthermore, the conclusions and recommendations made are based on the information and analysis available to us at the time of writing. If the facts change, our opinions and recommendations may alter also.

Executive Summary

Castlebridge have prepared this research report for the purposes of supporting Data Protection Impact Assessment activity in respect of contact tracing apps and associated mobile device-based interventions in public health response to pandemic scenarios or other infectious disease outbreak scenarios.

Since the first edition of this research report, which focussed on the implementation of contact tracing in Singapore, there has been extensive further research in this area and critical assessment of the suitability of the technology approaches proposed. In addition, there has been the development of a number of frameworks for centralised and decentralised processing of Bluetooth identifiers to support contact tracing, and Apple and Google have collaborated on a technical API standard to address many of the operational issues that have affected previous generations of contact tracing apps from the dim and distant past of mid-March 2020.

Outline of Methodology

Castlebridge applied a variant of our Data Protection Impact Assessment/Ethical Impact Assessment methodologies to the analysis of a set of defined use cases derived from media discussion of various uses for smartphone/mobile phone data to support covid-19 response initiatives.

In doing so, we have drawn on our international network of experts in data protection, telecommunications, and clinical data study design, as well as individuals with personal experience of some of the applications discussed, to develop the best possible analysis. The business needs/use cases we identified for analysis in this report are set out below.

Business Need	Summary Approach
Identification of Close Contacts and support for contact tracing	Use mobile phone data (location or other) to identify close contacts and support contact tracing.
Provide symptom tracking and recording to support epidemiological data capture/analysis	Provide a smartphone app where users can log symptoms they are experiencing.
Notify individuals if they have had close contact with someone who has tested positive	Send push notification from smartphone app to notify the person who has been in close contact
To track population movements to support analysis/prediction of disease trends and effectiveness of containment	Use mobile phone data to identify movements people
Provide information to app users	Use push notification to give targeted information to app users

Summary of Conclusions and Recommendations

Our conclusions and recommendations are summarised below.

Contact Tracing

Since the first edition of this research report, which focussed on the implementation of contact tracing in Singapore, there has been extensive further research in this area and critical assessment of the suitability of the technology approaches proposed. In addition, there has been a rapid pace of development in respect of protocols to implement a technical approach to support contact tracing. Based on our review of the published information at this time, we recommend:

1) Pragmatism and clear management of expectations in respect to the effectiveness and accuracy of BT-LE as a means for measuring proximity is essential. While it is better than other technologies and is potentially the most privacy preserving technology currently available, it is being implemented to do something the protocols were not developed to do and there are significant technical challenges that need to be recognised.

2) Adoption of a decentralised Exposure Notification/Contact Tracing application strategy based on DP-3T, with an intent to implement the Apple/Google API. It is our assessment that this provides the best balance against the data protection rights of individuals and the obligations of organisations. There is a clear roadmap for supporting interoperability across borders, and the mechanisms for processing apply the data minimisation principle and avoid disclosing the social graph of any individual. Additional data capture can be implemented at the application level, subject to a valid legal basis and a DPIA.

   With the implementation of the Google/Apple API as a decentralised exposure notification solution that addresses at operating system level many of the challenges regarding battery life and, in the latest iteration, accuracy of proximity calculations, it is difficult to see how a centralised architecture that cannot implement these features in their application without impacting user experience or battery life could be implemented without impact on user adoption.

   Furthermore, with several EU member states abandoning centralised architectures in favour of DP-3T based frameworks, future interoperability

could become problematic for Centralised approaches (as required under EDPB Functional Requirement FUNC-5).

3) Any DPIA should distinguish between the process of identifying Bluetooth Identifiers (what Apple/Google now term 'Exposure Notification') and the other potential data requirements of a contact tracing process. Consideration should be given to explicit use cases that define the business need and approach through the life cycle of the data.

4) The design of any application should consider the User Personas who will interact with it. Consideration should be given to the potential impacts on children, persons with diminished capacity, or other vulnerable persons.

5) Push notifications should be implemented with caution and in a manner that supports existing manual contact tracing but does not replace it. Consideration should be given to how inbound versus outbound calls to action will be implemented, and processes should be designed accordingly. Furthermore, any messages should be prepared in a way that is intelligible to all potential categories of user, taking into account age, literacy, and other factors

6) The EDPB guidance on the requirements for contact tracing applications are quite clear and should be considered and applied in any DPIA. Note that this may require domestic legislation to give effect to appropriate safeguards for data and for fundamental rights.

   The application should have the sole purpose of contact tracing (see recommendations re: Application strategy below).

   Applications should be voluntary, and any additional data processed must be for a specific and lawful purpose. Authorities should avoid any suggestion that an application is "mandatory but not compulsory" in the user experience that is being implemented.

   Applications should be open-source and the technical specifications made public. Furthermore, there needs to be evaluation of effectiveness from a public health perspective with defined KPIs for measuring effectiveness.

7) Transparency is essential during the design and development of any application. Furthermore, it is a key success factor in implementation and adoption by communities.

8) Contact tracing should preserve the “human touch” in design and execution of processes, particularly for vulnerable persons, children, or persons with diminished capacity.

9) A clear contact centre strategy is required. While inbound calling by individuals is the most privacy preserving, outbound calling may be a more appropriate mechanism. Both bring with them issues. A potential solution is a hybrid model supporting inbound and outbound calling. Process design is an essential aspect of ensuring optimal outcomes. This should also include consideration of how to ensure validation of outbound calls from Public Health Authority to mitigate risk of malicious callers.

Symptom Tracking

Symptom tracking apps provide a potentially rich source of epidemiological data relating to the progression of the illness. They may also provide data to help differentiate the symptoms of other commonly occurring illnesses from those of Covid-19.

There are potential issues of data quality in the context of self-reported symptoms and also consistency of completion of self-reporting which could impact the effectiveness of logged data.

We recommend that they be deployed as a “second wave” application in the context of contact tracing to support the management of close proximity contacts of infected persons. This will help reduce the “noise” in the data that is gathered and will enable causation and correlation factors to be more readily identified. This is in line with the EDPB Functional Consideration FUNC-1 in their guidance on Contact Tracing Apps.

We also make a number of high-level recommendations regarding the security of data in such applications.

We advise that self-reported symptoms should not be used as a trigger for exposure risk notification/contact tracing alerts due to the subjectivity of the data and the risk of it being maliciously abused. This increases the risk of “alert fatigue”.

An exception to our recommendations regarding symptom tracking would be the use of clinically prescribed remote monitoring / telemedicine solutions to support diagnosed or suspected cases of Covid-19 who are self-isolating. We believe these have a potentially significant value in an overall system optimisation approach to the pandemic response.

Push Notification of Close Contact

It is questionable if the push notification of a close proximity contact to a person who has tested positive is **necessary** to protect the vital interest of the data subject or another or if it is **necessary** to pursue the public health objective.

It is also possible that push notifications could cause unnecessary distress to data subjects and, absent appropriate context in communication, could trigger unexpected and undesirable consequences for third parties. Consideration should also be given to the risk of 'Alert Fatigue'.

In particular, the risk of sending a push notification to a child, or to a vulnerable person, cannot be ignored.

Push notifications should be a supplement to and not a replacement for existing contact tracing and follow up protocols. It is essential that the "human touch" is not lost.

Furthermore, consideration should be given to the "next action" that would be taken by persons in receipt of a push notification. Any action that results in a substantial increase in calls to local primary care facilities should be avoided. Likewise, if the call to action is to contact a central number, this must be adequately resourced to ensure callers are answered in a timely manner and ideally on their first attempt.

Analysis of Population Movement using Mobile Data

Analysis of population movement using mobile data represents a significant risk of mass surveillance and would require either processing on the basis of consent or the processing of anonymised data.

A range of very clear safeguards would be required to balance data protection and data privacy obligations against the objectives of processing this data.

It is important to note that the data is of insufficient granularity to support contact tracing but would, in an aggregate form, potentially support measurement of effectiveness of social controls on movement.

Push Notifications to App Users

Push notifications of a general information nature to app users have a lawful basis either on the basis of consent or on the basis of processing in the public interest.

We would question the need for these to be implemented as part of an application or application framework and would recommend instead that an SMS subscription service where people can subscribe for general updates would be enough to meet the need of general communication.

Application Strategy

We recommend against the development of a single application to perform multiple functions given the potential for complexity which may impact usability and acceptance of the application. This is echoed in the EDPB guidance on Purpose Limitation in the context of Contact Tracing applications (PUR-1)

Where a single app/multiple functions strategy is adopted, there should be a clear application roadmap indicating what functionality will be enabled when, and under what circumstances/in response to what triggers.

Ultimately any application must be seen in the context of the overall response system. In that context, any barriers to adoption should be minimised and explicit consideration should be given to how the applications interact with and support existing public health response processes such as contact tracing, testing, and hospital care.

The implementation of an application should be considered in the wider context of rapid testing and other infection control methods and should not be the primary focus of any infection control strategy.