Speak for Yourself!
Attitudes to contact tracing applications in the context of COVID-19: results from a nationally representative survey of the UK population

Professor Carsten Maple (University of Warwick), cm@warwick.ac.uk

Dr Rebecca McDonald (University of Birmingham), R.L.McDonald@bham.ac.uk

Version v1.0

18 May 2020

For later versions contact the authors

Contents

Executive Summary

1. Background
   1.1 There is an ongoing debate in the public arena about the use of app-based contact tracing to help manage the COVID-19 pandemic. A number of countries have deployed contact tracing techniques to address the spread of the disease. A trial of a centralised UK app is ongoing on the Isle of Wight.
   1.2 Despite controversy around what approach is in the public's best interest, as yet, the opinions of the public have not been gathered, analysed or considered at a representative scale.
   1.3 We have undertaken a nationally-representative survey of the UK public. We utilised a specific method, a Discrete Choice Experiment (DCE), to help understand public opinion on aspects of contact tracing apps.
   1.4 The purpose of this work is to help inform those intending to design and deploy contact tracing apps in time of pandemic, **allowing governments to make appropriate design choices to ensure adequate uptake and participation**. In cases where concern exists, but a government has an overriding requirement, the **insights can inform awareness and informational campaigns, to increase understanding of the design choice.**
   1.5 We present here the key initial findings of the work.

2. Discrete choice experiment: paired choices between hypothetical apps, with option to opt out.
   2.1 Of all participants, 9.6% always chose to **opt out** of using a contact tracing app.
   2.2 There is no significant (negative) impact of any location data (GPS, wifi or mobile signal strength) being used alongside proximity data (Bluetooth).
   2.3 Linking proximity data to any other data sources reduces acceptability of contact tracing. (In order of unacceptability: shopping location from credit/debit cards; travelcard; phone or social network contacts; name and address).
   2.4 The recipient of any shared anonymised data determines acceptability of the app. Sharing data with **other app users is the least acceptable**. Sharing with **NHS is the most acceptable**, followed by with researchers, and then national and local government. The DP3T approach is decentralised, so only other users receive the information, whereas the NHSX app uses a centralised approach in which the (anonymised) information on those with COVID is held centrally and not distributed.
   2.5 **Older people** and those on **higher incomes** are significantly **more likely** to say they are willing to use the app. We find no effect of gender or education level.
   2.6 Technologically engaged people, (typified in this case by those who tend to leave Bluetooth switched on, and those who have engaged with an app or web-based COVID reporting tool) are **more likely** to opt in.
   2.7 Those still regularly leaving home during lockdown (e.g. for work) are **less likely to opt in**.

3. General willingness to opt in to a contact tracing app
   3.1 When asked "Overall, if a contact tracing app became available today, would you download and use it?", **66.4% of participants said they probably or definitely would download it**, compared with 17.6% saying they would probably or definitely not. In the DCE, participants were willing to use the app in 74.3% of choices

4. Practicalities
   4.1 We explored practical concerns that have been raised around what a contact tracing app might require to run effectively. We found some concern over the impact on phone **battery**, the amount of **data** it might require, and whether the app must be open in the **foreground** of the mobile phone. Whilst the use of Bluetooth was a cause for concern for some participants, it was the least problematic of the practicalities that we investigated.

5. Risk
   5.1 Reidentification: Participants were most concerned about the possibility that **other users** could reidentify them. 53.0% of participants reported moderate or extreme concern about this, compared to 15% expressing concern about reidentification by the NHS.
   5.2 Sharing additional data: We used an example case of **partial postcodes**, which feature in the NHSX app trial. In general, participants were not very concerned about sharing this information (74.3% of participants were "not at all" or "slightly" concerned).

6. Oversight and control
   6.1 Appropriateness of oversight: By far the most popular candidate for oversight of the app was the **NHS**, with 81.9% of participants stating this would be completely or somewhat appropriate. Participants did not clearly distinguish between the three other candidates (an independent group of advisory technology experts (GATE), or local or national government).
   6.2 Willingness to share information: We explained that an app user who was notified that they had COVID-19 would be asked to share an anonymised list of the people the app recognised they had had contact with. We elicited participants' willingness to share this list with each of four types of recipient: local government, national government, NHS and researchers. Again, **participants favoured the NHS**, with 84.2% probably or definitely being willing to share. Sharing with researchers was more acceptable than with local or national government.
   6.3 Participants are slightly **more concerned about what data is shared**, than about who it is shared with, but that they are slightly **more likely to opt out based on the recipient of the data**. Respectively, 64.0% of participants think it very or extremely important to have control over what data is shared, whilst 61.4% think it very or extremely important to control who it is shared with.

7. Trust in organisations
   7.1 We elicited the degree to which participants trust different agencies with their data. Specifically, we asked them to rate their agreement with statements intended to measure trust in each organisations' intentions and capabilities related to data use and data security. The **most trusted was the NHS**, followed by researchers. Local and national government were not clearly distinguished, and were less trusted overall than either NHS or researchers.
   7.2 In addition, we explored whether participants would trust the technology companies that provide the technology underpinning the app. Of our participants, **61.6% believed Apple and Google would be somewhat or extremely likely to access the data for other reasons**, compared to just 12.4% who say it is somewhat or extremely unlikely. This level of distrust is much more pronounced than the distrust in government.

8. Trade-off between privacy and effectiveness
   8.1 Deciding the acceptable level of intrusiveness in a contact tracing app, requires understanding how society balances concerns about privacy against controlling the spread of the pandemic.
   8.2 We asked participants if "We should prioritise privacy, even if this means not controlling the pandemic as effectively" or "We should prioritise controlling the pandemic, even if this means that privacy is compromised". **57.4% of participants slightly or strongly favoured prioritising controlling the pandemic over privacy. Conversely, 20.1% slightly or strongly favoured protecting privacy over controlling the pandemic.**

Background

Severe Acute Respiratory Syndrome Coronavirus-2 (SARS-CoV-2) is a novel strain of the coronavirus disease first detected in humans in 2019. The outbreak was declared a Public Health Emergency of International Concern by the World Health Organisation (WHO) on 30 January 2020, and on 11 February the WHO announced they would refer to the disease as COVID-19. Figures from the WHO, as of 17 May 2020, indicate that there were 4,525,497 confirmed cases of COVID-19 globally, resulting in 307,395 deaths (WHO, 2020).

Contact tracing is a technique that has previously been applied to control outbreaks of infectious diseases. In a recent paper in the Lancet, researchers from London School of Hygiene & Tropical Medicine (Hellewell, 2020) ran a series of simulations and concluded that "highly effective contact tracing and case isolation is enough to control a new outbreak of COVID-19 within 3 months." A number of countries have already deployed contact tracing techniques to address the spread of COVID-19, including Singapore, South Korea and Australia. Manual contact tracing was used in Singapore, supported by the development of a mobile phone app. While manual contact tracing can be effective it is not scalable and a reliable contact graph cannot be established when the identity of a contact is not known to the person reporting symptoms. As such, there has been a great deal of effort in developing technology-based solutions.

A significant group of academics in Europe came together to create a method that could be deployed across Europe, allowing interoperability and coordination across the Union. The initiative was termed the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) project. However, a subgroup of the researchers became increasingly concerned that the team were not "sharing the protocols, the code and the thinking" as well as the fact that the approach was centralised and, as such, required a trusted third party to receive information. This subgroup created the Decentralized Privacy-Preserving Proximity Tracing (DP3T) approach. A rather unedifying and public battle ensued with each criticising the other's approach. On April 10, Apple and Google announced they would come together to develop a combined API and eventual system-level contact tracing feature. The approach would align with the DP3T approach and be decentralised. On April 30, NHSX in the UK announced they would not use the Apple-Google approach but rather develop a centralised approach, and has now deployed a trial on the Isle of Wight.

With all of the possible design choices for a contact-tracing app, many commentators and experts have argued which approach is in the best interests of the public. For example, some have argued that centralised apps create privacy invasions that are unacceptable; others have argued that to be effective the apps should be centralised. However, as yet, the opinions of the public have not been gathered, analysed or considered at a representative scale. It is this omission that we address in this paper – we let the public speak for itself. To facilitate this, we have undertaken a nationally-representative survey. Of course, we recognise that the public are not necessarily experts, and may act in self- rather than societal-interest. Further, any contact tracing design should include input from a wide range of experts, including those from health and infectious diseases, law, ethics, behavioural psychology, security, privacy, systems engineering and more besides. However, we do believe that the public voice should be heard, and it is this we attend to achieve here.

Our survey is representative across age, gender, income and educational attainment. In our survey, 93% of respondents reported that they use a smart phone. This is comparable to the recently reported statistic that 96% of adults in the UK own a mobile phone (Statista, 2019).

Our survey design included questions to examine hypotheses inspired by examining the literature surrounding the methods that were being proposed as a basis for deployment, studying peer-review and commentary of the proposed methods, and analysing commentary and analysis of real deployments of contact-tracing apps such as in Singapore, South Korea and Australia. The flagship part of our study consists of a Discrete Choice Experiment, designed to reveal insights about public opinion on the type of data used, identifiably of individuals, who data access was granted to, and the period for which data was to be held and used.

The purpose of this work is to help inform those intending to design and deploy contact tracing apps in time of pandemic. We provide insights into those aspects of an app that the public feel uncomfortable about, or make them disengage from participation. This will allow governments to make appropriate design choices to ensure adequate uptake and participation. In cases where concern exists, but a government has an overriding requirement, the insights can inform awareness and informational campaigns, to increase understanding of the design choice.

This draft presents the initial analysis and results, and will be updated as more sophisticated analysis is completed.

Methods

Discrete choice experiment methodology

Part 1 of the survey was a Discrete Choice Experiment (REF). This methodology involves pairwise choices between options described in terms of their characteristics ('attributes'). Analysis of these choices provides a quantitative estimate of the relative importance of the attributes. In our study, participants made 12 choices between pairs of hypothetical contact tracing apps.

These hypothetical apps were described by six attributes, which were characteristics that may plausibly influence the acceptability or uptake of the contact tracing app. These attributes included the sensitivity of the app, the data it would require, who would have access to the data, how long data would be stored for, and the degree to which the data could be used to personally identify the user. Each of these attributes took one of a number of levels. Table 1 presents a full description of the attributes and levels.[1] In each choice, participants selected their preferred app (we asked "Which app do you prefer") and had the option to "opt out" of using either app (we asked "Is your preferred app better than no app at all?).[2]

Participants' choices between the different hypothetical apps with different combinations of levels reveals the relative importance of each characteristic, and provides a rich account of the acceptability of a potential contact tracing app for the UK population.

[1] We employed a D-efficient design to select combinations of attributes and levels for the survey. This ensures that the parameters are efficiently estimated. We used STATA's dcreate command (Hole, 20XX) to generate 100 choice pairs which were organised in 10 blocks of 12 choices. Participants were randomised into blocks, and the choices within each block were shown in a random order.

[2] Prior to answering the twelve questions, participants were introduced to the concept of a contact tracing app, and all six attributes were described to them. They completed two warm up tasks prior to the twelve main questions. At the end, an additional DCE choice was included as an attention check. It differed only in its effectiveness. Any participant selecting the less effective app was automatically filtered out of the survey

To analyse the DCE data, we employed a logistic regression with an alternative-specific constant. The coefficients can be interpreted as marginal utilities, assuming a random utility model (McFadden XX). We use the efficiency attribute (number of cases identified out of 100 that should be) as a numeraire to make the other attribute estimates comparable.

Table 1 Attributes and levels underpinning the discrete choice experiment

Attribute	**Levels [X]**
Sensitivity "Of every 100 app users who come into contact with someone with COVID-19, [X] of them will be notified"	85 90 94 97 99
Data types (proximity/location) "The app will use [X] to identify who you have been near"	Bluetooth Bluetooth and wifi Bluetooth and GPS Bluetooth and your mobile network signal Bluetooth, wifi, GPS, and your mobile network signal
Data types (other) "The app will link [X} with your proximity and location data	No additional data Your name and address Your shopping location from your debit/credit card data Data from your contactless travel card/app Contacts from your mobile phone or social networks
Recipients "Your data will be shared with [X]"	Other app users only Your local or regional government The national government The NHS Researchers studying the spread of infections
How the sharing happens "Your data will be shared in a way that means [X]"	You can be personally identified You can be identified as belonging to a certain group You cannot be identified
Time "Your data will be stored [X]"	for up to 1 week for up to 2 weeks for up to 4 weeks for up to 6 months until end of pandemic

Survey methodology

Part 2 of the survey elicited participants' attitudes towards aspects of the contact tracing applications. We included questions in four broad categories. The first was practicalities, such as how much data it would require, whether it would need to be open in the foreground of the phone, and how it would influence battery life. The second category was risk, such as the risk of being re-identified, and the risk of false positives. The third category elicited opinions about who should have oversight of the app, and whether participants would be willing to share relevant information with different authorities and organisations. The fourth category explored trust, including trust in government, NHS, researchers, and tech companies. We also captured their overall subjective estimate of how likely they

would be to download and use a contact tracing app if it were available immediately; and their perceived trade-off between the importance of privacy versus controlling the pandemic.

The attitudinal questions were recorded using five-point Likert scales. We typically described an issue and asked a subset of the following questions: how concerned the participant would be about the issue; how important they considered the issue to be; how much they agreed or disagreed with a statement about the issue; and/or how likely they would be to choose not to use the app due to this issue. For simplicity, much of the analysis of the five-point Likert scales treats the data as cardinal.

In addition to the attitudinal questions, we recorded participants' sociodemographic information (see Table 2), their current level of engagement with smartphone and app technologies (**Table 3**), and how they had been, or felt they might be, affected by COVID-19 (Table 4).

Details about the specific questions asked are detailed in the results section of this report, and screenshots of the full questionnaire are available.

Sample

Demographics

In total, 2,171 members of the UK general population took part in the survey. The sample was recruited by Qualtrics and was selected to be representative on age, gender, geographic location, educational attainment, and household income before tax. Sociodemographic sample statistics are presented in Table 2. We also asked about contactless travelcard use because data from this technology is included in some choices in the DCE.

Table 2 Socio-demographic characteristics

Socio-demographic characteristics	
Gender (%)	
Male	48.2
Female	51.4
Other	0.3
Age (years)	
Mean (s.dev)	44.6 (17.4)
Pre-tax household income (GBP)	
Mean (s. dev)	39,345 (31,569)
Self-reported deprivation scale (%)	
Living comfortably	17.4
Doing alright	39.1
Just about getting by	26.7
Finding it quite difficult	10.3
Finding it very difficult	6.5
Highest educational attainment (%)	
Primary school	0.7
Secondary school	23.8
6th form or college	38.9
UG degree	24.1
Masters degree	8.7
PhD	2.2
Other	1.8
Use of contactless travelcard (%)	
Yes	37.4
No – don't use contactless	13.6
No – don't use public transport	49.0

Engagement with technology

We elicited participants' degree of engagement with technology, particularly focusing on their smartphone use, use of apps and Bluetooth. Results are presented in Table **3**. The vast majority of participants (92.9%) in our sample use a smartphone. Only 2.5% of respondents stated that they did not know what Bluetooth was, and just over half of respondents tend to leave Bluetooth switched on. Whilst 83.4% of the sample reported regularly using smartphone apps, just 9.0% of them have downloaded a COVID-related app, or used the web to report COVID-related symptoms.

Table 3 Engagement with smartphone technology

Question	%
Do you use a smartphone?	
Yes	92.9
No	7.1
Do you tend to leave Bluetooth switched on?	
Yes	51.1
No	46.5
I don't know what Bluetooth is	2.5
Do you regularly use apps on your smartphone?	
Yes	83.43
No	16.44
Have you already downloaded any apps related to COVID-19 or used the NHS symptom reporting website?	
Yes	8.97
No	91.03

COVID-19 experience and attitudes

We measured participants' perceptions of their personal risks related to COVID-19, and the results are given in Table 4. Of our sample, 8.4% had a confirmed or suspected case of COVID-19. A substantial minority of our sample reported being at high risk of COVID-19 (23.0%), and 7.2% had been identified by government as being vulnerable. Just under 20% of the sample reported still leaving home regularly during lockdown, for example going to work, 34.8% of all respondents reported their work having been affected by COVID-19, with this rising to 43.7% of those in work at the beginning of the pandemic. When asked whether they would take a test if it was available now, 72.8% responded favourably.

Figure 1 illustrates this attitude.

Figure 1 "Would you like to take a test for COVID-19 if it was available for you?

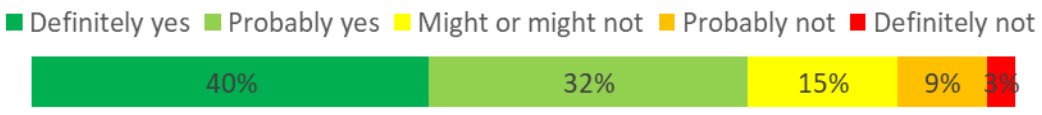


Table 4 Perceptions, characteristics and behaviour related to COVID-19

Question	%
Had, or think have had COVID-19	
Yes	8.4
Unsure	10.4
No	81.2
Government identified as clinically vulnerable	
Yes	7.2
No	92.8
Self-identified as high risk	
Yes	23.0
No	77.0
Regularly leaving home (e.g. for work) during lockdown	
Yes	19.8
No	80.2
Job had been affected by COVID-19	
Yes	34.8
No	44.4
Not applicable (not in work before outbreak)	20.8

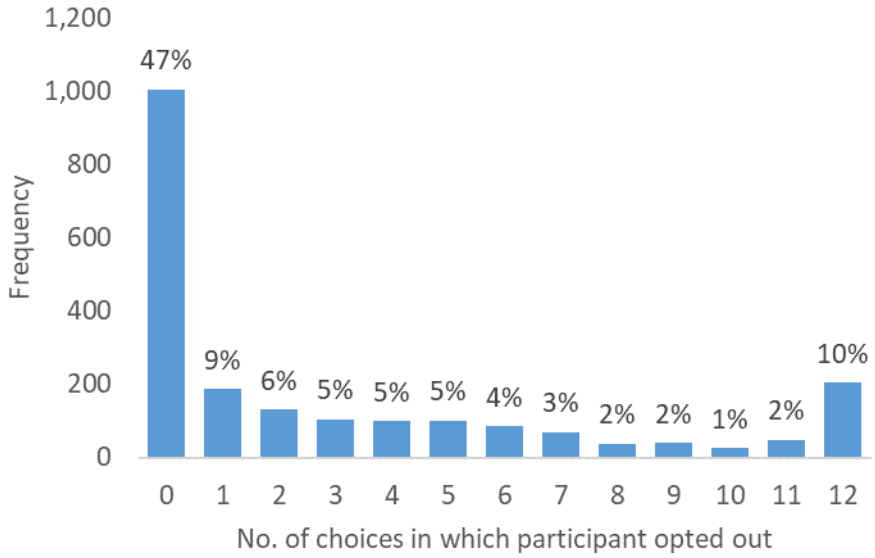
Attitudes to contact tracing: discrete choice experiment results

This section reports the results of the Discrete Choice Experiment. First we consider how many participants stated that neither app is acceptable to them (i.e., they chose to opt out). Then we turn to the main results of the DCE, looking at the relative importance of the attributes. Finally, we consider the demographic and other characteristics, as well as some attitudes measured elsewhere in the survey, and how these predict uptake of a contact tracing app.

Opting out

First we consider the responses to the question "is your preferred app better than no contact tracing app at all". There are two interpretations of the answer "yes" to this question. First, the participant may think that the particular apps in that choice are not good enough to opt into. Second, the participant may never be willing to opt in to a contact tracing app. To distinguish these cases, we count the number of times each participant chose to opt out. The results are presented in Figure 2. 46.8% of participants always considered their preferred app to be better than no app at all. 9.6% always selected the opt out, and may be considered to be protest respondents. The remaining 43.6% have between 1 and 11 opt outs, and the frequency of these is relatively evenly distributed.

Figure 2 Opting out in DCE choices



DCE results

Main attributes

The results of the DCE is presented in Figure 3 and Figure 4 Additional controls in analysis of the DCE. The DCE was analysed using an Alternative-Specific Constant Logit in Stata. The figure reports relative risk ratios with 95% confidence intervals. Full regression models are in Appendix 1. Figure 3 gives odds ratios associated with each level of each attribute in the DCE.

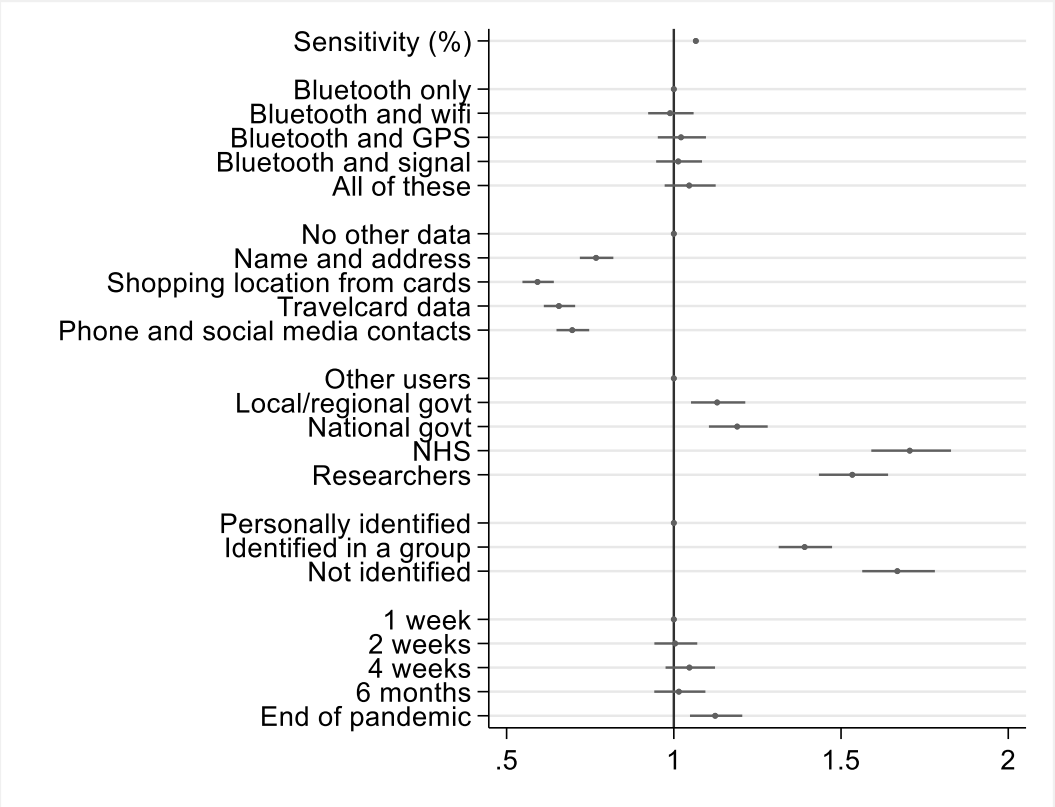
Sensitivity

Apps with better sensitivity were more popular, with a 1% increase in sensitivity corresponding to a 6.6% increase in the likelihood of opting in to using the app. This is significant with $p<0.001$. In addition to providing a sense check, the app's sensitivity acts a numeraire through which we can compare the relative importance of the other attributes.

Location data

In addition to the proximity information provided by Bluetooth, the hypothetical apps in the DCE may use location data to help identify contacts. We found remarkable indifference to the use of location data in addition to proximity data. None of wifi, GPS, or mobile network signal significantly altered the likelihood that an app is chosen, and sharing all three location data types was not significantly different than sharing none of them.

Figure 3 Main attributes of the DCE. The DCE was analysed using an Alternative-Specific Constant Logit in Stata. The figure reports odds ratios with 95% confidence intervals. Full regression models are in Appendix 1.



Other data

Respondents were much more concerned about linking wider data types. The data types selected are ones that can supplement proximity-based contact tracing, and have variously been proposed or used in previous contact tracing trials. Each of the tested data types reduced respondents' willingness to select the app. The item with greatest concern was "shopping location based on your credit and debit card data", followed by contactless travelcard data, then phone or social media contacts, and name and address was the datatype participants were the least concerned about. All pairwise comparisons are significant with $p<0.001$. [3]

Data recipient

We varied the recipient of the anonymised list of contacts in the event that the app user is notified as having COVID-19. This attribute captures the distinction within centralised models between those who would handle the data (government, NHS or researchers). It also broadly captures the distinction between centralised and decentralised models, in the comparison of "other app users only" (as in a decentralised model) and the rest of the levels (as in centralised models). Our results are firmly in favour of a centralised model. Other app users sharing the data is deeply unpopular, and reduces the likelihood that the app is selected relative to all other models ($p<0.001$ in all comparisons).

We can also distinguish between the recipients of the data. The most preferred is the NHS: respondents were 70.5% more likely to opt in to an app if the NHS was the recipient, compared to if other users were the recipients. The next preferred option is researchers, with 53.4% higher likelihood

[3] With a Bonferroni correction, significance drops for the comparison between contacts and name and address ($p=0.052$) and the comparison between shopping location data and travelcard data ($p=0.058$)

of opting in, compared to other users. National government and local or regional government were the least preferred recipients in centralised models, with respondents 13.0% and 19.0% more likely to opt in with each of these recipients respectively, compared to other users. All comparisons are significant with $p<0.001$ except for the levels of government which are statistically indistinguishable from one another.

Identifiability
Respondents had a clear preference for their data to be used and shared in a way that meant they could not be personally identified. From a baseline of being personally identified, being idenitified only as part of a group raised the odds that the app is selected by 39.1%, and not being identified at all raises it by 66.8%. All pairwise comparisons are statistically significant ($p<0.001$).

Duration that data is held
A concern with the centralised models is the length of time for which data is held. Respondents appeared not to be concerned about this. In comparison to an app that stores their data for 1 week, raising this to 2 weeks, 4 weeks, or 6 months is not statistically significantly different. In fact, apps in which data is stored until the end of the pandemic were *more* popular than those that store it for up to one week. Respondents were 12.4% more likely to opt for an app storing their data until the end of the pandemic, than one that stores it for up to one week. This difference is statistically significant ($p=0.01$).

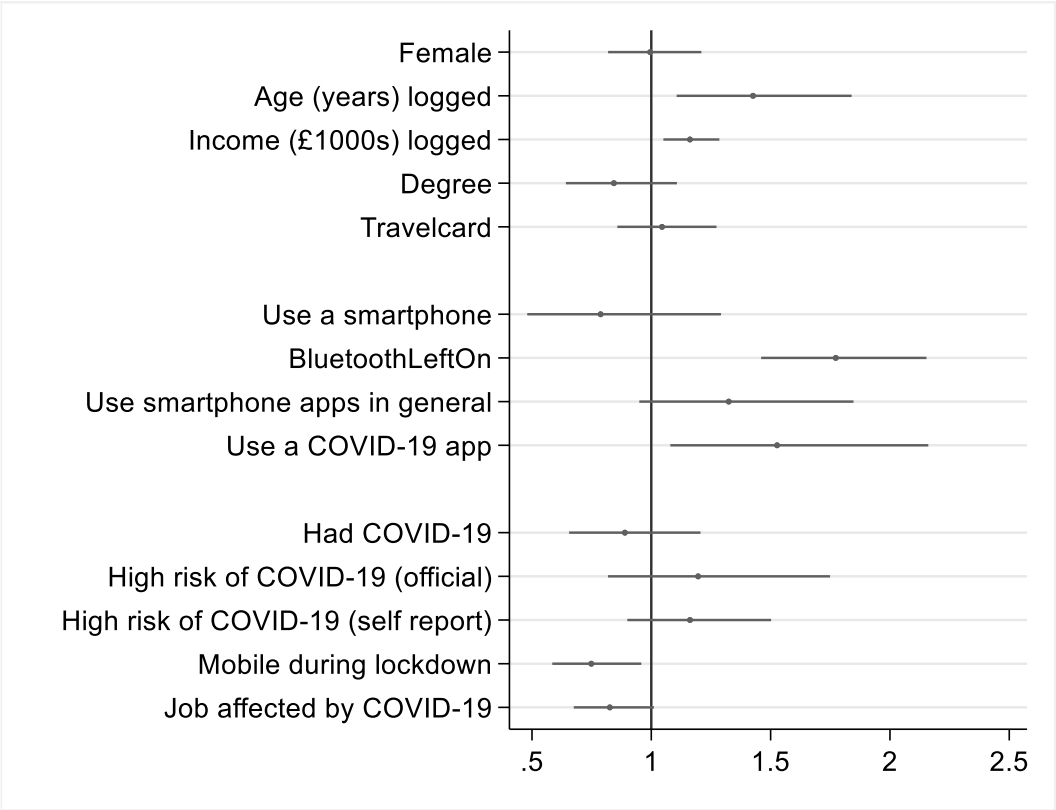
Other explanatory variables in the DCE

Sociodemographics
Being older, and having a higher income, are both associated with a significant positive increase in the likelihood of opting in to using the contact tracing apps in the DCE. The figure shows logged variables to best demonstrate the effects, but the regression models in Appendix 1 show that a £1000 increase in income is associated with an increase of 4.0% in the likelihood of opting in, whilst being one year older is associated with a 1.0% increase in the likelihood of opting in. We find no effect of gender, education, or use of a contactless travelcard (relevant for the linked data attribute in the DCE).

Engagement with smartphone technology
Opting in to the app was more common amongst those participants that tend to leave Bluetooth switched on (81.9% more likely to opt in, $p<0.001$), and those who have already downloaded a COVID-19 app or used a website to report COVID-19 symptoms (53.1% more likely to opt in, $p=0.016$). However, we found no effect of whether a person uses smartphone apps in general, and we do not find an overall effect of smartphone use.

Experience with COVID-19
There is a negative association between uptake of the app and whether the respondent is still leaving home regularly during lockdown. A person still leaving home is only 76.7% as likely to download the app as someone not regularly leaving home. This association is significant ($p=0.096$). However, having had COVID-19, being at higher risk of COVID-19, or having income affected by COVID-19 are not associated with the likelihood of opting in to the use of these apps.

Figure 4 Additional controls in analysis of the DCE. The DCE was analysed using an Alternative-Specific Constant Logit in Stata. The figure reports relative risk ratios with 95% confidence intervals. Full regression models are in Appendix 1

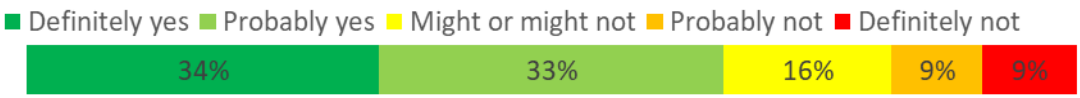


Attitudinal results

General willingness to opt in to a contact tracing app

We asked "Overall, if a contact tracing app became available today, would you download and use it?". The response was largely favourable, with 66.4% of respondents saying the probably or definitely would, compared with 17.6% saying they probably or definitely would not download it. However, 66.4% is arguably lower than the required proportion, and so it will be important to persuade the 16.0% undecided people to opt in if the app is to be effective.

Figure 5 Willingness to opt in to a contact tracing app



Practicalities

We explored some of the practical concerns that have been raised around how a contact tracing app might work, and what it might require in order to run effectively. This included its toll on battery life, the amount of data it might use, and whether it must be open in the foreground of the mobile phone in order to work. In each case, we explored how concerned people are about this aspect of the contact tracing app, as well as how likely they would be to decide against using the app due to this issue.

We told respondents that the app may mean their phone might lose its charge faster than usual. 49.6% of participants stated that they were somewhat or extremely likely to decide against using the app due

to its effect on their battery life. There was slightly more concern about the possibility of the app needing to open in the foreground of the phone, and yet the implications for uptake were weaker. This may reflect that foregrounding is a security concern, that participants were willing to trade off against the benefit from using the app, whilst the battery issue is not a concern in the same way, but may present a practical barrier for uptake. Figure 8 and Figure 9 display that participants are concerned about the impact of the app on their data, especially if it requires a large amount (70MB) of data per day. In this case, 47% of respondents report being somewhat or extremely likely to decide against using the app, so data concerns have a greater impact on potential uptake than the security concern around having to keep the app in the foreground of the phone.

Figure 6 Battery life

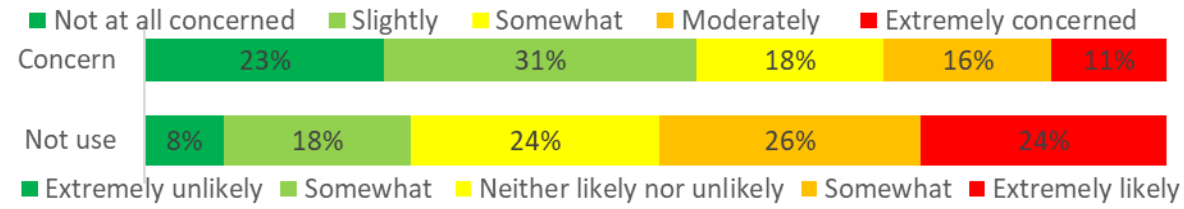


Figure 7 Foregrounding

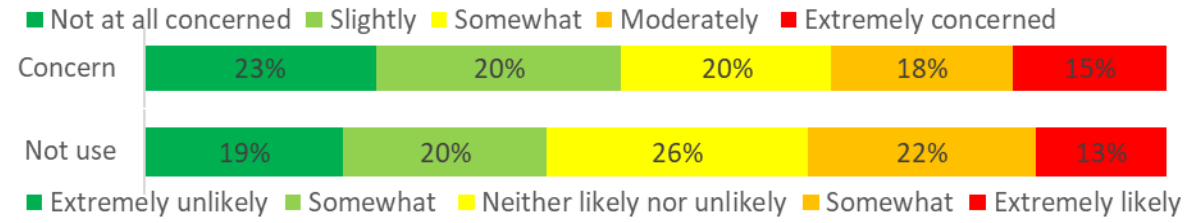


Figure 8 Using 70MB per day of data

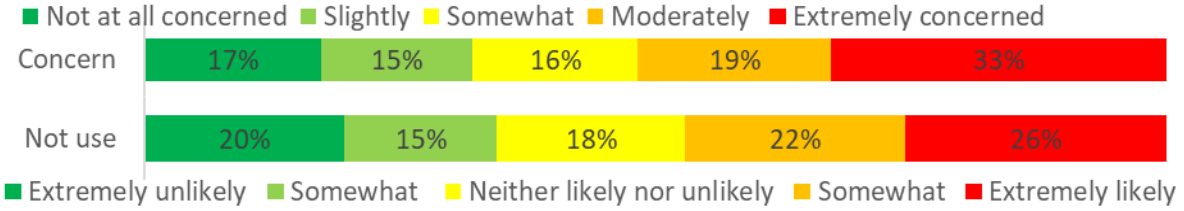
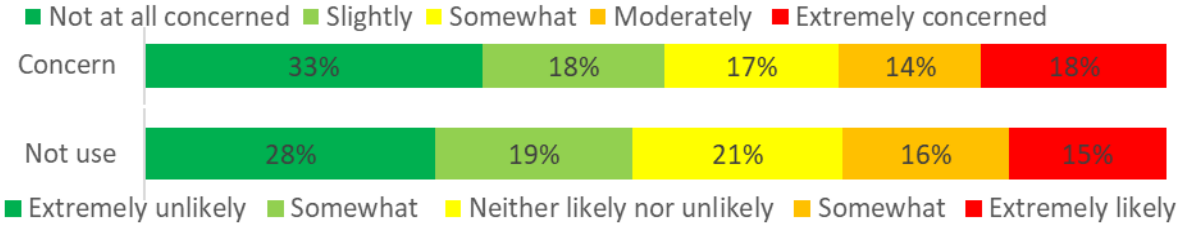
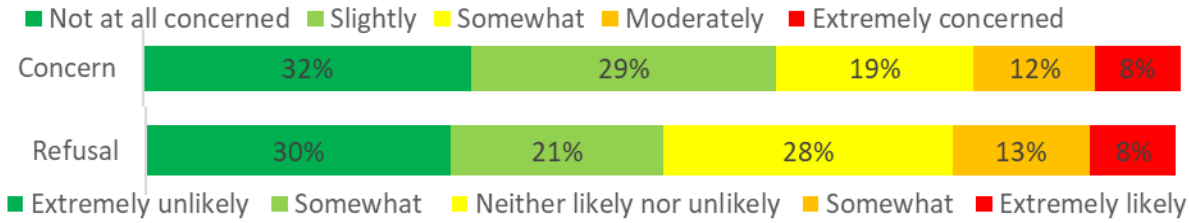


Figure 9 Using 3MB per day of data



The use of Bluetooth is a requirement for almost any proposed contact tracing app. This was a cause for concern for some participants, but the refusal to use the app due to the use of Bluetooth was relatively low, with 21.7% of respondents either somewhat or extremely likely to decide not to use it for this reason. Bluetooth was the least problematic of the practicalities that we investigated.

Figure 10 Using Bluetooth to identify proximity

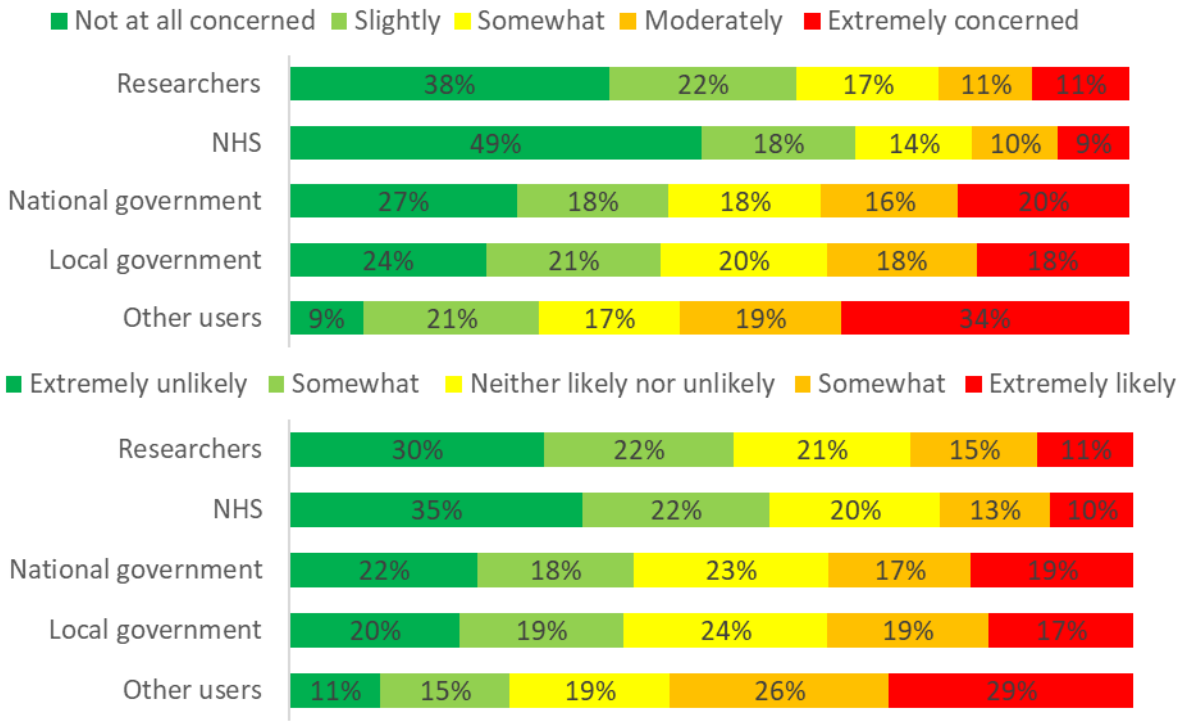


Risks

Reidentification

Using a contact tracing app will carry some risks to the user, including risks of being reidentified, risks of false positives, and some risks that come from the possibility of information being leaked. To explore this, and to introduce the idea of *who* might access the information held in the app, we first asked respondents to state their degree of concern and their likelihood of opting out from the app due to the possibility of reidentification by each of four potential user groups that could, in principle, access the data. Participants were most concerned about the possibility that other users could reidentify them, and this led to 55.0% of participants stating they were somewhat or extremely likely to opt out. Concern was lowest for NHS, then researchers, with reidentification by local or national government relatively frequent cause for concern.

Figure 11 Reidentification

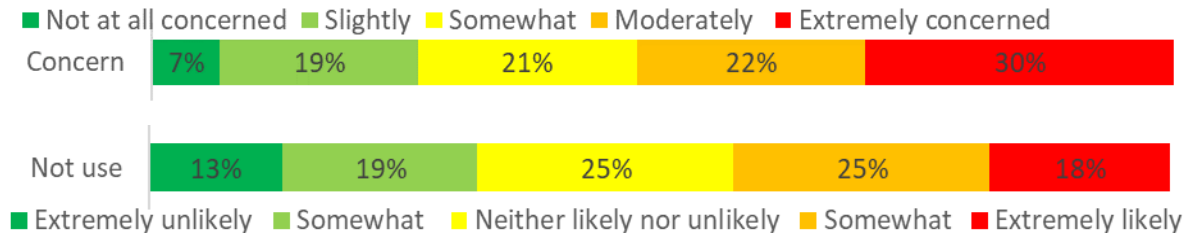


False positives

There is a risk of false positives, where the app notifies the user, perhaps indicating that they should self-isolate, when in fact no positive contact has been made. We briefly explained the idea of false positives to respondents and elicited their opinions about them (see Figure 12). Participants saw false positives as a major cause for concern, with 30.3% of participants reporting being extremely concerned. This is second only to their concern about reidentification by other users of the app.

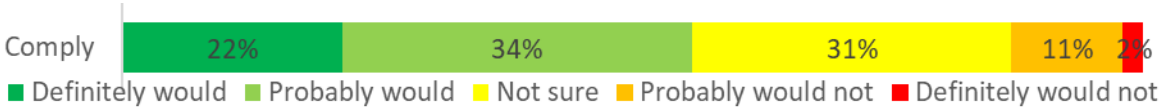
Overall, 43% of respondents thought they would be somewhat or extremely likely to decide not to use the app due to the risk of false positives.

Figure 12 False positives



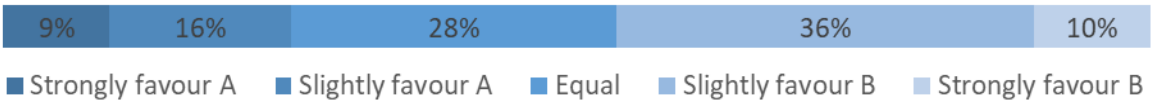
To further explore the issue of false positives, we asked respondents how likely they thought they would be to self-isolate in a circumstance where the app recommended this, but they doubted that they had made any contact with others. Respondents reported high levels of compliance, with well over half (55.8%) reporting that they probably or definitely would self-isolate, even if they thought the app was mistaken. This may explain the high level of concern about false positives, due to the anticipated disruption they would cause.

Figure 13 Comply with recommendation



Finally, we explored how people would balance the trade-off between false positives and false negatives. We proposed two apps: app A has few false positives, but was more likely to miss real cases of contact, whilst app B has many false positives, but was less likely to miss real cases of contact. Participants tended to favour app B, indicating that although they are concerned about false positives, they would be willing to incur some risk of these if the app is more effective at identifying real cases of contact.

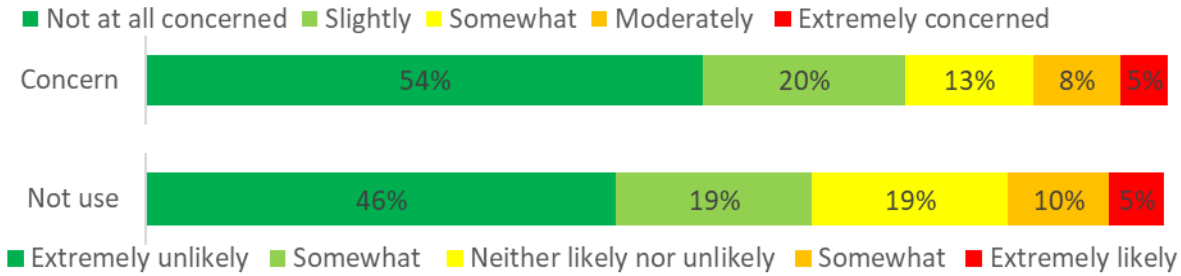
Figure 14 Trade-off between false positives and false negatives



Postcode

To capture whether participants would be concerned about sharing potentially personal information, we used an example case of partial postcodes. This is a useful testbed since the UK's NHS contact tracing app requests this information at present. We did not mention the likelihood of this data being misused. Instead, we simply asked "The app may require you to share the first part of your postcode in order to run". In general, participants were not very concerned about sharing this information, with 74.3% of participants being "not at all" or "slightly" concerned.

Figure 15 Sharing first part of the postcode

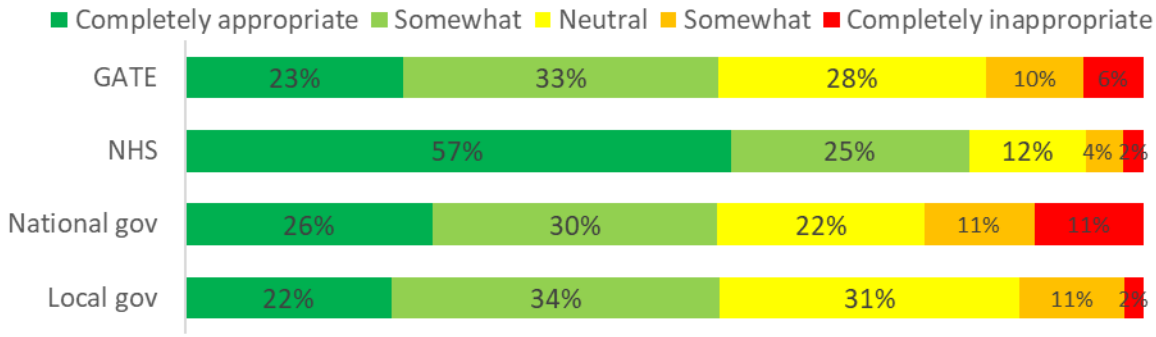


Oversight and control

Appropriateness of oversight

At the heart of the debate around the UK's contact tracing app is the question of who should have oversight. We proposed four agencies to our respondents and they rated the degree of appropriateness they perceived to apply in each case. By far the most popular candidate was the NHS, with 81.9% of respondents stating this would be completely or somewhat appropriate. They did not very clearly distinguish between the three other candidates of an independent group of advisory technology experts (GATE), or local or national government. There was a notable absence of support for the oversight of the independent group, suggesting that if such a group was established it must seek to gain the trust of the public in this role.

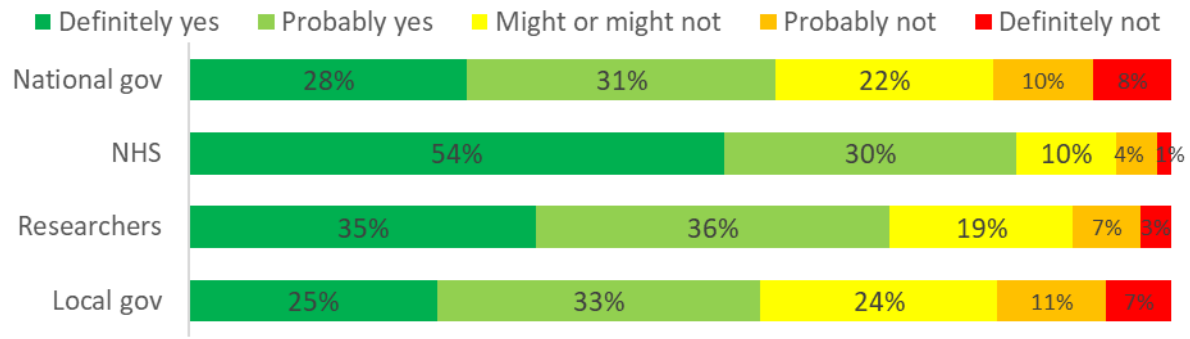
Figure 16 Oversight appropriateness



Willingness to share contact information by recipient

In the survey, we explained that if an app user was notified that they had COVID-19, they would be asked to share an anonymised list of all the people the app recognised they had had contact with. We elicited participants' willingness to share this list with each of four types of recipient: local government, national government, NHS and researchers. Again, participants favoured the NHS, with 84.2% probably or definitely being willing to share. Sharing with researchers was more acceptable than with government. Again, national and local government were not strongly distinguished.

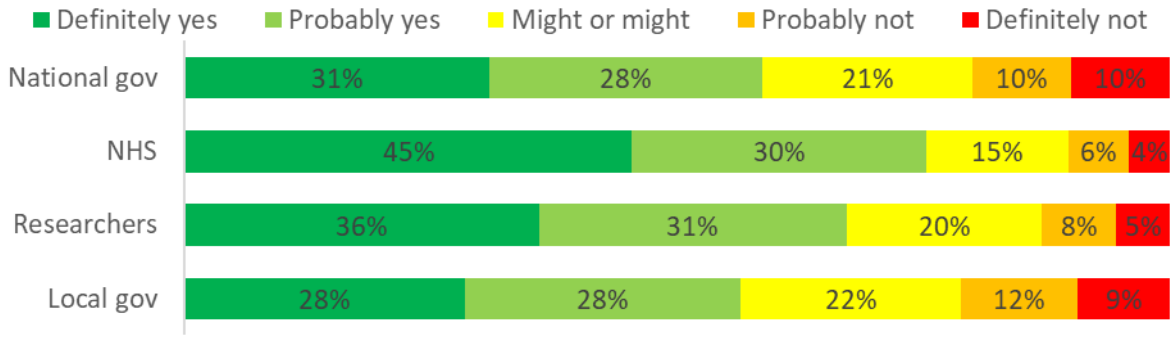
Figure 17 Willingness to share anonymised list of contacts



Willingness to share overseas travel information by recipient

The app may not work abroad, and if not then this may mean app users needing to report when they have left the country and/or download another app that works overseas. We explored the acceptability of sharing overseas travel information with the same four recipients, and we asked whether respondents would be willing to download another app for use overseas. There was a slightly lower willingness to share travel data than contact data, which could reflect that respondents see a less direct link between sharing that type of data and the app's purpose.

Figure 18 Willingness to share infromation about overseas travel



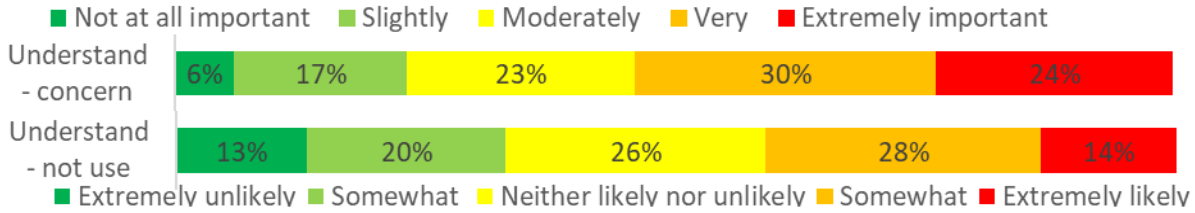
The app being developed in the UK is unlikely to be compatible with apps developed in Europe. As such, contacts from overseas cannot be shared. We examined whether participants would be willing to download an app in an overseas country. Willingness to download an alternative overseas app was subdued, with just 43.7% of respondents either probably or definitely willing to download the overseas app, and the proportion unsure (29.8%) was relatively large compared to other questions.

Figure 19 Willingness to download an overseas contact tracing app

Importance of understanding the technology

Previous research has shown that some participants feel it is important to understand technology that has implications for their privacy. Over half of participants (53.9%) said it was very important or extremely important for them to understand the technology, whereas just 23.2% said it was slightly important or not at all important. This concern feeds through to a reluctance to use the app: 41.1% of participants said they were somewhat or extremely likely not to use the app if they did not understand how it works, compared to 32.9% who said it was somewhat or extremely unlikely that they would opt out for this reason.

Figure 20 Understanding the technology



Importance of control over what information is shared and with whom

Participants often express a desire to retain control over their data and personal information. We tested two aspects over which they might have or relinquish control: what data is shared, and who it is shared with. We find that people are slightly more concerned about what data is shared, than about who it is shared with, but that they are slightly more likely to opt out based on the recipient of the data. Respectively, 64.0% of participants think it very or extremely important to have control over what data is shared, whilst 61.4% think it very or extremely important to control who it is shared with. In terms of opting out of using the app, 48.9% of participants consider themselves somewhat or extremely likely to opt out if they had no control over what data was shared, compared to 50.5% who would opt out if they had no control over who it is shared with.

Overall, the patterns suggest that understanding the app is the most important of these concerns, followed by having control over what happens to the data.

Figure 21 Control over what data is shared

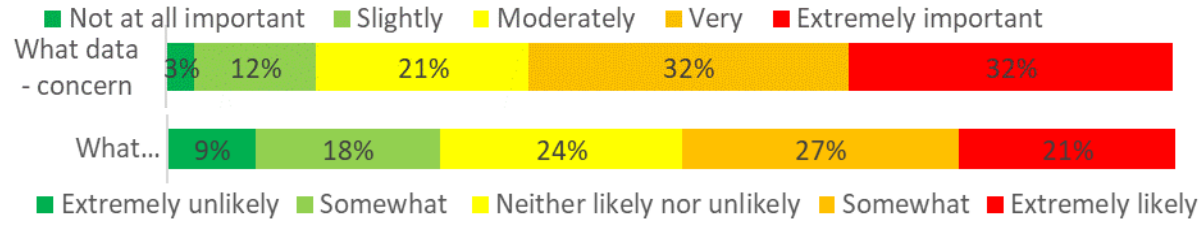
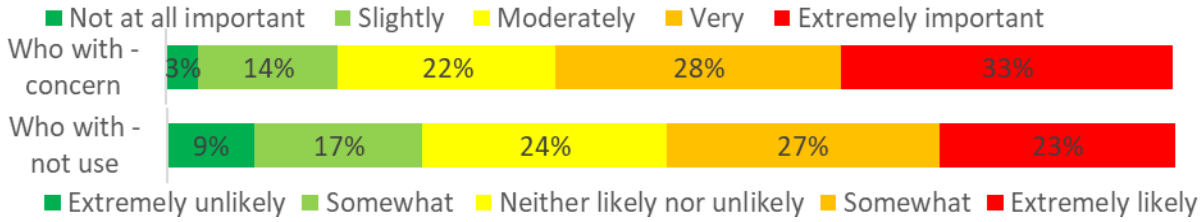


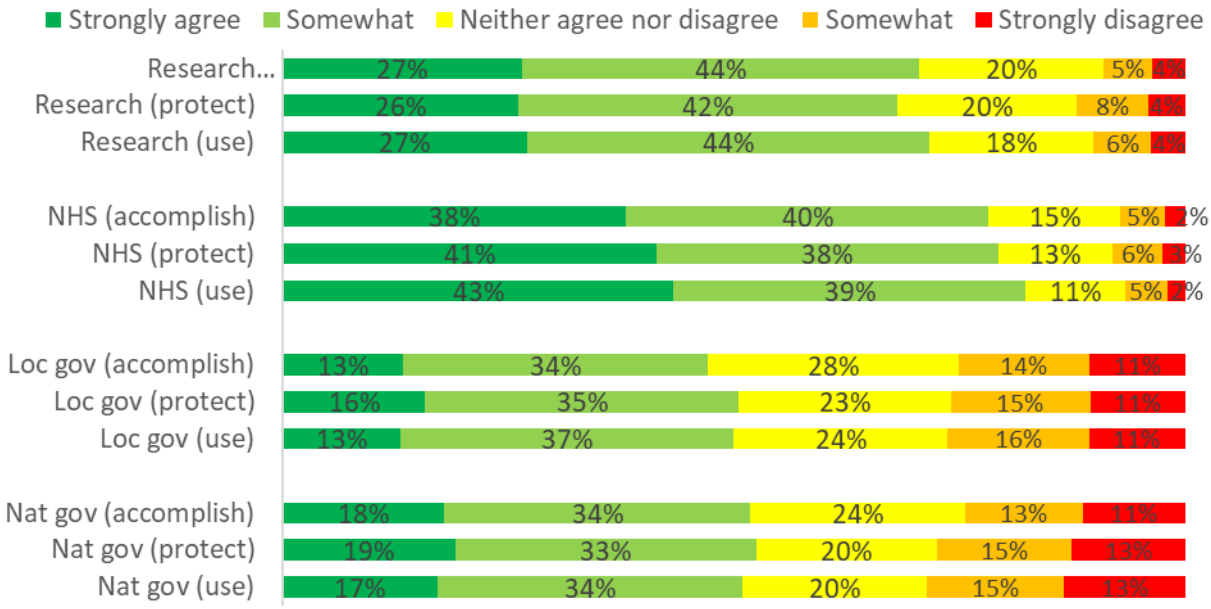
Figure 22 Control over who data is shared with



Trust in organisations

Results from the Discrete Choice Experiment, as well as from the reidentification concerns and willingness to share data in the attitudinal survey, suggest that participants have clear preferences over who their data is shared with. To understand this, we elicited the degree to which participants trust different agencies with their data. Specifically, we asked them to rate their agreement with three statements. The first was “I trust [organisation] to use my personal data only for the purposes of contact tracing”. The second was “If my data is sent to [organisation], I trust them to protect it”. The third was “I believe [organisation] have the ability to accomplish what they say they will do with my data”. These three statements relate to their trust in the intentions of the organisation (statement 1), as well as their processes (statement 2) and their competence (statement 3). We repeated the question for national government, local government, the NHS, and researchers.

Figure 23 Trust in organisations



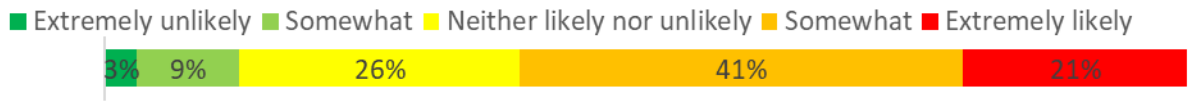
Government, NHS and researchers

The results support the interpretation that the earlier results were driven by trust in the various organisations. The most trusted was the NHS, followed by researchers. Local and national government were not strongly distinguished, and were less trusted overall than either NHS or researchers. There were no clear differences between the different facets of trust, with very little variation between statements about intentions, protection, or their capacity to accomplish the stated aims. Figure 23 illustrates the responses.

Technology companies

In addition to the bodies that may oversee any contact tracing app, we wished to explore whether participants would trust the technology companies that provide the technology underpinning the app. Specifically, we stated "You may have heard that Apple and Google are creating some technology to support contact tracing apps. How likely do you think it is that they will access the contact tracing app data for other purposes?" The results show a striking lack of trust in these companies, with 61.6% of participants believing these companies were somewhat or extremely likely to access the data for other reasons, compared to just 12.4% who say it is somewhat or extremely unlikely. This level of distrust is much more pronounced than the distrust in government.

Figure 24 Trust in technology companies



Tradeoff between privacy and effectiveness

In the wider debate about the level of intrusiveness acceptable in a contact tracing app, there is an important matter of principle. This is, how should society balance concerns about privacy against controlling the spread of the pandemic? Knowing how members of the public would answer this question is important for understanding the normative stance that policy should take, helping to ensure the appropriate balance is struck to respect the preferences of the population. It is also of practical

importance, since it has implications for the uptake of the app and for public support for, and compliance with, wider policies in this area.

Figure 25 Prioritising controlling the pandemic or protecting privacy

We provided two statements, each representing an opposite extreme stance in this debate. Participants told us how they would balance the two statements, either strongly favouring one over the other, slightly favouring one, or equally favouring them. The statements were "We should prioritise privacy, even if this means not controlling the pandemic as effectively" and "We should prioritise controlling the pandemic, even if this means that privacy is compromised". The degree of support for these statements is shown in Figure 25. Support for controlling the pandemic was common, with 57.4% of participants slightly or strongly favouring this. However, the preference was by no means unanimous. 75.1% of respondents indicated at least some concern for privacy, and 20.1% slightly or strongly favoured protecting privacy over controlling the pandemic.

Discussion

This study gives a comprehensive, contemporaneous snapshot of the attitudes to issues around contact tracing apps in the UK population in the context of the COVID-19 pandemic. The work was inspired by the contention surrounding contact tracing apps and the lack of a public voice in the discussion. The survey and DCE were based on an analysis of the literature surrounding methods that were being proposed as a basis for deployment; peer-review and commentary of the proposed methods; and analysing commentary and analysis of real deployments of contact-tracing apps such as in Singapore, South Korea and Australia.

The initial analysis identifies a number of key areas to consider if an app is to be trusted and used by the public in the UK. In particular, we have found that the public want to ensure that any app that is deployed is effective. Apps that are currently proposed are based on Bluetooth to establish whether individuals have been in close contact by identifying the proximity of their devices; this approach does not require the location of an individual to be known or recorded. Respondents, somewhat surprisingly, have no concerns over whether location data is also collected by the app. However, using other types of data, such as shopping location from credit/debit cards, contactless travelcard data, phone or social network contacts, or name and address caused concern to participants.

There has been a lot of discussion in the mainstream and technology press regarding the use of centralised versus decentralised approaches. The latter removes government, or other bodies, having access to data and taking an active role in the system. This has privacy benefits, which has been a core motivation behind efforts by the DP3T community. In their system, only other users would have access to anonymised data of those that had contracted the disease. This approach is contrary to the system being trialled by NHSX, which clearly believes the benefit of accessing the data outweighs any privacy incursions (of course, the app is not mandatory). When respondents were asked about who they would prefer to receive anonymised data, sharing data with other app users is actually, somewhat surprisingly, the least acceptable. Sharing with the NHS is the most acceptable, followed by sharing with researchers, and then national and local government. This demonstrates the amount of

trust that users place in the NHS (perhaps especially salient given the current situation), but also, surprisingly, the lack of trust in sharing with other individuals.

We proposed four agencies to have oversight of the use of the technology. By far the most popular candidate was the NHS, with 81.9% of respondents stating this would be completely or somewhat appropriate. Surprisingly, the use of an independent Group of Advisors on Technology in Emergencies, as proposed by the Ada Lovelace Institute [Lovelace, 2020] was much-less favoured than the NHS, and not clearly distinguished in favourability from government. To understand these results, and those of the DCE, we examined participant trust in organisations and again it was clear that the NHS enjoyed overwhelming trust. Researchers were trusted only slightly less, but there was more scepticism of local and national government. Given that Apple and Google have announced that they will provide interfaces for contact tracing apps, we examined whether these companies enjoyed citizen trust. 61.6% of participants believe that Apple and Google would be somewhat or extremely likely to access the data for other reasons. The authors recognise, that for a variety of reasons it is highly unlikely that this would happen in practice, and so were surprised at the level of distrust.

Any app being developed would great benefit in terms of engagement if it afforded a level of control to the user. 64.0% of participants think it very or extremely important to have control over what data is shared, whilst 61.4% think it very or extremely important to control who it is shared with.

In addition to governance issues, we have explored a variety of practical issues involved in running the app, and have found that phone battery, the amount of data it might require, and whether the app must be open in the foreground of the mobile phone were all issues that should be considered in the design of the app. The use of Bluetooth was of no or only of slight concern for more than half the respondents. The NHSX app trial required users to share the first part of their postcode and this was not seen as problematic to respondents; 74.3% of participants were “not at all” or “slightly” concerned about this.

Our discussion so far has focused on how the characteristics of an app and its governance can make people more or less likely to choose to use it. However, the characteristics of individuals matter significantly in predicting uptake. Our results suggest that older people and those on higher incomes are significantly more likely to use the app, and technologically engaged people, (typified in this case by those who tend to leave Bluetooth switched on, and those who have engaged with an app or web-based COVID reporting tool) are more likely to opt in. However, those still regularly leaving home during lockdown (e.g. for work) are less likely to opt in. This is a concern as those regularly leaving home are likely to meet more people than those not. This indicates that there is a need for a more sophisticated holistic approach to managing and identifying the contacts of those that contract the disease. There is a need for a number of initiatives, such as a supporting information and awareness campaigns, and restrictions imposed in public spaces, in addition to a technology-based approach to effectively manage the pandemic. Our work indicates that if an app were available today, 66.4% of people “probably or definitely would” download it, compared with 17.6% who would “probably or definitely not”.

One of the main motivations for this work was that there has been a significant discussion on the balance between privacy and the national interest in effectively addressing the pandemic. We asked participants whether they thought it more important to prioritise controlling the pandemic or to protecting privacy, 57% indicated that preferred controlling the pandemic, while 21% preferred protecting privacy. This clearly demonstrates that the public are willing to sacrifice some of their privacy if it meant that the app was more effective in controlling the pandemic. This consideration should be respected in the development of any solution that is deployed in the UK.

Appendix 1: Regression output from DCE

VARIABLES	Model(1)	Model(2)	Model(3)	Model(4)
SENSITIVITY (% OF TRUE POSITIVES NOTIFIED)	1.064***	1.065***	1.065***	1.066***
	(0.00255)	(0.00266)	(0.00272)	(0.00312)
WHAT PROXIMITY/ LOCATION DATA IS USED? (BASELINE = BLUETOOTH ONLY)				
Bluetooth and wifi	0.969	0.986	0.990	0.989
	(0.0281)	(0.0295)	(0.0306)	(0.0346)
Bluetooth and GPS	1.010	1.010	1.015	1.022
	(0.0301)	(0.0311)	(0.0321)	(0.0367)
Bluetooth and mobile signal	1.031	1.032	1.040	1.013
	(0.0296)	(0.0306)	(0.0317)	(0.0350)
All of the above	1.011	1.010	1.016	1.046
	(0.0308)	(0.0317)	(0.0328)	(0.0389)
WHAT OTHER PERSONAL DATA IS USED? (BASELINE = NONE)				
Name and address	0.756***	0.763***	0.762***	0.767***
	(0.0206)	(0.0215)	(0.0221)	(0.0255)
Shopping location from cards	0.614***	0.616***	0.609***	0.592***
	(0.0203)	(0.0211)	(0.0215)	(0.0239)
Travelcard data	0.663***	0.668***	0.662***	0.656***
	(0.0200)	(0.0207)	(0.0212)	(0.0239)
Contacts (phone or social media)	0.702***	0.710***	0.707***	0.696***
	(0.0208)	(0.0218)	(0.0223)	(0.0249)
WHO IS THE DATA SHARED WITH? (BASELINE = OTHER APP USERS)				
Local or regional government	1.154***	1.155***	1.156***	1.130***
	(0.0357)	(0.0366)	(0.0375)	(0.0414)
National government	1.156***	1.168***	1.173***	1.190***
	(0.0365)	(0.0380)	(0.0393)	(0.0448)
The NHS	1.704***	1.712***	1.720***	1.705***
	(0.0508)	(0.0523)	(0.0539)	(0.0607)
Researchers	1.499***	1.525***	1.527***	1.534***
GRANULARITY OF IDENTIFICATION (BASELINE = PERSONALLY IDENTIFIABLE)	(0.0434)	(0.0454)	(0.0468)	(0.0527)
Identified at a group level	1.415***	1.421***	1.421***	1.391***
	(0.0348)	(0.0360)	(0.0368)	(0.0407)
Not identified	1.703***	1.697***	1.684***	1.668***
	(0.0459)	(0.0475)	(0.0486)	(0.0554)
HOW LONG IS THE DATA STORED FOR? (BASELINE = 1 WEEK)				
2 weeks	0.998	1.014	1.006	1.004
	(0.0268)	(0.0280)	(0.0285)	(0.0327)
4 weeks	1.023	1.038	1.039	1.047
	(0.0298)	(0.0312)	(0.0322)	(0.0377)
6 months	0.994	1.012	1.004	1.015

	(0.0310)	(0.0326)	(0.0335)	(0.0389)
Until the end of the pandemic	1.105***	1.121***	1.109**	1.124**
	(0.0329)	(0.0345)	(0.0350)	(0.0399)
SOCIO-DEMOGRAPHICS				
Age (years)		1.009***	1.013***	1.010**
		(0.00242)	(0.00271)	(0.00349)
Female		0.950	0.981	0.999
		(0.0787)	(0.0836)	(0.0997)
Household pre-tax income		1.000***	1.000***	1.000*
		(1.61e-06)	(1.62e-06)	(1.85e-06)
UG degree or higher		0.828	0.820	0.855
		(0.0985)	(0.0996)	(0.119)
Use a travelcard			1.069	1.045
			(0.0923)	(0.105)
USE OF SMARTPHONE TECHNOLOGY				
Use a smartphone			0.844	0.795
			(0.183)	(0.202)
Leave Bluetooth on			1.627***	1.769***
			(0.140)	(0.176)
Use apps			1.318+	1.372+
			(0.187)	(0.237)
Use a COVID app			1.585**	1.533*
			(0.234)	(0.270)
COVID-19				
Confirmed or suspected coronavirus				0.896
				(0.140)
Identified as vulnerable				1.192
				(0.231)
Self-reported high risk				1.137
				(0.149)
Leaving home during lockdown				0.762*
				(0.0958)
Job affected by pandemic				0.841+
				(0.0868)
CONSTANT	1.888***	0.983	0.601+	0.793
	(0.111)	(0.153)	(0.160)	(0.256)
Observations	77,328	72,900	69,408	53,460
LL	-26664	-24951	-23575	-18030
Cases	25776	24300	23136	17820
Clusters	2148	2025	1928	1485

Robust standard errors in parentheses; *** p<0.001, ** p<0.01, * p<0.05, + p<0.1

References

[WHO, 2020] *Coronavirus disease (COVID-19) Situation Report – 118*. World Health Organisation. Accessed 17 May 2020 from https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200517-covid-19-sitrep-118.pdf?sfvrsn=21c0dafe_6

[Hellewell, 2020] Hellewell, J., Abbott, S., Gimma, A., Bosse, N.I., Jarvis, C.I., Russell, T.W., Munday, J.D., Kucharski, A.J., Edmunds, W.J., Sun, F. and Flasche, S., 2020. *Feasibility of controlling COVID-19 outbreaks by isolation of cases and contacts*. The Lancet Global Health.

[Statista, 2019] *Mobile phone usage in the United Kingdom (UK) 2005-2018*. Statista. Accessed 18 May 2020 from https://www.statista.com/statistics/300378/mobile-phone-usage-in-the-uk/

[Lovelace, 2020] *COVID-19 Rapid Evidence Review: Exit through the App Store?* Ada Lovelace Institute. Accessed 18 May 2020 from https://www.adalovelaceinstitute.org/wp-content/uploads/2020/04/Ada-Lovelace-Institute-Rapid-Evidence-Review-Exit-through-the-App-Store-April-2020-2.pdf

[Louviere, 2000] Louviere, J. J., Hensher, D. A., & Swait, J. D. *Stated choice methods: analysis and applications*. Cambridge university press.