Ada Lovelace Institute

Rapid evidence review
20 April 2020

Exit through the App Store?

A rapid evidence review on the technical considerations and societal implications of using technology to transition from the COVID-19 crisis

This rapid evidence review sets out proposals for whether, and how, the UK Government should use technology to transition from the COVID-19 global public health crisis.

It examines the potential development and implementation of technical solutions to support symptom tracking, contact tracing and immunity certification. In doing so, its analysis takes into account societal, political, legal and ethical perspectives, and gives findings and recommendations for the transition and rebuild phases that follow containment, delay and mitigation.

Key takeaways

For Government

- There is an absence of evidence to support the immediate national deployment of the technical solutions under consideration.
- Effective deployment of technology to support the transition from the crisis will be contingent on public trust and confidence, which can be strengthened through the establishment of two accountability mechanisms: the Group of Advisors on Technology in Emergencies (GATE) to review evidence, advise on design and oversee implementation, and an independent oversight mechanism to conduct real-time scrutiny of policy formulation.
- Clear and comprehensive primary legislation should be advanced to regulate data processing in symptom tracking and digital contact tracing applications. Legislation should impose strict purpose, access and time limitations.
- Until a robust and credible means of immunity testing is developed, focus should be on developing a comprehensive strategy around immunity that considers the deep societal implications of any immunity certification regime, rather than on developing digital immunity certificates.

For Parliament

- Primary legislation is required to impose strict purpose and time limitations on technical solutions to support transition from the crisis.
- Primary legislation will be required to govern any future regime of immunity testing and certification. Such a regime will have deep societal implications and it will be critical that it is subject to robust and expert debate and scrutiny in Parliament.

For technology providers and developers

- The rushed deployment of technical solutions without credible supporting evidence and independent oversight may undermine public trust and impede the effectiveness of the implementations in supporting the crisis response.
- Technical design choices should take into account the need to factor in privacy-by-design and accessibility features, and should be buttressed by non-technical measures to account for digital exclusion.

Executive summary

Governments around the world are beginning to look to data-driven technologies as tools to support the transition from emergency lockdown measures in response to COVID-19.

The UK is facing a bleak and worsening economic forecast, raising pressure to make moves to restart the economy and reassure the markets. As the initial emergency measures become normalised, both the public and opposition parties are beginning to call for clarification on Government plans to transition from complete lockdown as the country passes the first peak of the virus. Current global consensus is that the return to pre-pandemic movement can only be achieved in the long-term by vaccination (with a timescale of more than a year). In the UK adequate levels of testing and the capacity for manual tracking and isolation are not yet imminent.

The Government is right to explore non-clinical measures in its attempt to relax controls without an intolerable rise in COVID-19 cases. This shouldn't be critiqued as an attempt to weigh economic considerations against public health – there are very real societal risks on each side. Lockdown is giving rise to direct health risks (leaving vulnerable children without support and safeguards, exacerbating domestic abuse, mental health issues and suicides) as well as secondary health harms caused by a deep recession.

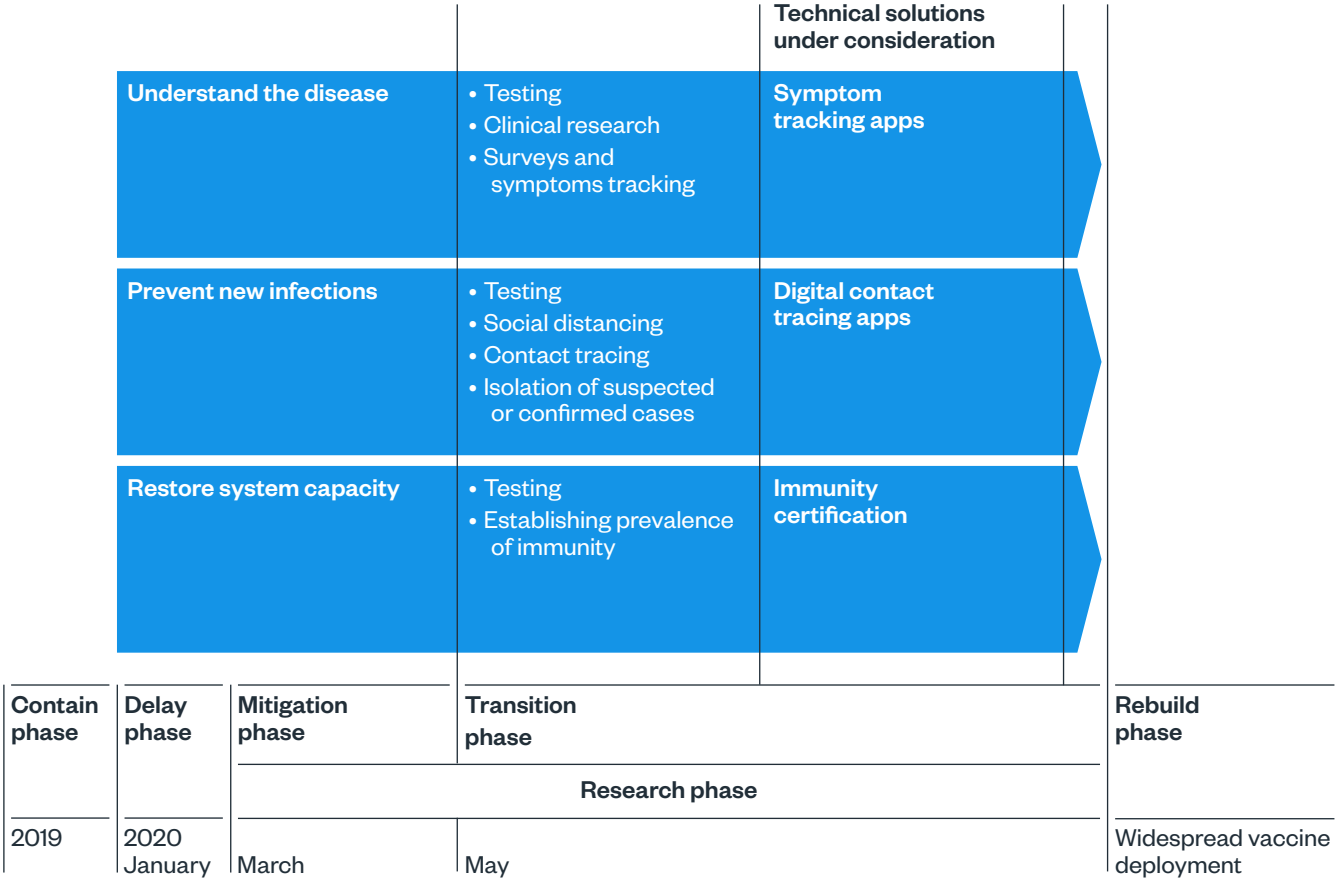

Chart 1
Overview of the uses of technology to transition from the COVID-19 crisis

There are three interlocking technical interventions under consideration in the UK, as well as in other countries around the world: symptom tracking applications, digital contact tracing applications and digital immunity certificates.[1] It is posited that these technologies can inform research into the disease, prevent further infections and support the restoration of system capacity and the opening up of the economy.

1 There are many others that are outside the purview of this review, including the use of technology to monitor and mitigate the spread of misinformation on social media platforms, such as: Ofcom. (2020). COVID-19 news and information: consumption and attitudes. *Ofcom.com*. Available from https://www.ofcom.org.uk/research-and-data/tv-radio-and-on-demand/news-media/coronavirus-news-consumption-attitudes-behaviour [Accessed 16.4.20].

There is a particularly urgent need to assess the efficacy and impact of digital contact tracing applications (Chapter 3), as one such application is presently under development by the NHS. Based on the current evidence in this review, the significant technical limitations, and deep social risks, of digital contact tracing outweigh the value offered to the crisis response. Overcoming these limitations and risks is not impossible but will require, at a minimum, that Government establishes a multidisciplinary Group of Advisors on Technology in Emergencies (GATE) to stand alongside the Scientific Advisory Group on Emergencies (SAGE) and act as gatekeepers of the deployment of technologies in support of a transition strategy.

Government should advance, and Parliament should adopt, primary legislation to bolster any eventual deployment of digital contact tracing apps, as well as to address concerns with symptom tracking applications (Chapter 4). Legislation should regulate but not require the use of digital contact tracing apps or symptom trackers; to make use mandatory on current evidence would not only undermine public trust and confidence, but likely fall foul of human rights standards.

Immunity certification (Chapter 5) should not be rolled out until accurate and reliable immunity tests exist, and until there is a robust understanding of the longevity and generalisability of immunity. If credible scientific evidence makes policy built around widespread immunity testing feasible, secure digital immunity certification may be feasible. However the accompanying interventions pose extremely high risks in terms of social cohesion, discrimination, exclusion and vulnerability. No immunity certification regime should be instituted in the absence of a comprehensive strategy that makes explicit the values that are being prioritised and those traded off, as well as primary legislation to underscore that strategy.

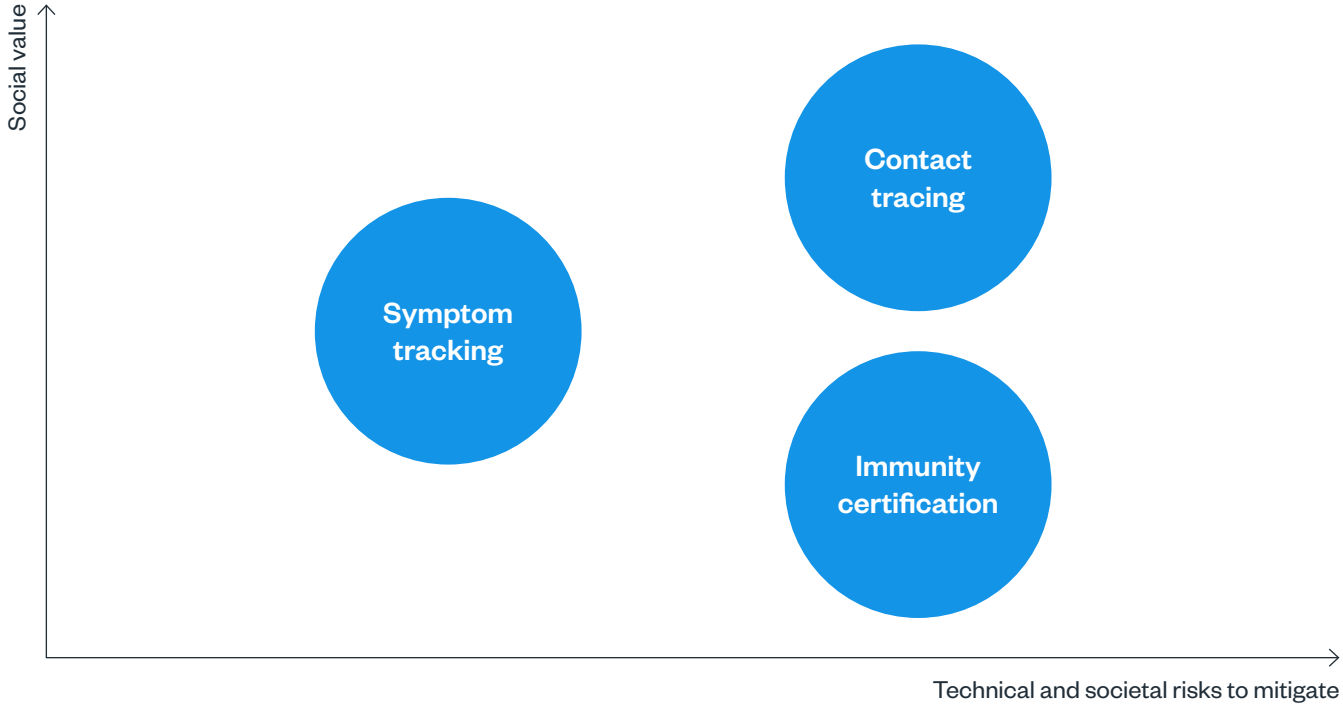

Chart 2
Weighing social value against technical and societal risks

Any exploration of data-driven mechanisms to support transition must be well-evidenced and deeply considerate of the societal and legal implications. Where the stakes are this high and the impacts so far reaching, Government must protect against the perception or reality of 'tech-solutionism', in which policy is led by technology, rather than the other way around.

We recommend two accountability mechanisms to bookend Government decision making – the establishment of the Group of Advisors on Technology for Emergencies to act as gatekeeper for the deployment of technical measures, and the establishment of an independent oversight mechanism to conduct real-time scrutiny of Government policy formulation.

Some technologies already in use or under consideration around the world have neglected to consider how technical design can serve efficacy and privacy, governance and transparency. The bar for technical solutions needs to be exceptionally high, open to scrutiny and oversight. Concerns about data exploitation and its knock-on harms could undermine public health and economy measures inexorably. Trust in responsible data governance in ways that are meaningful to the public has already been badly damaged, and yet will be critical to ensuring the success of technical interventions.

> **We call on Government to encourage privacy-by-design in technical implementations, and to advance primary legislation requiring symptom tracking and digital contact tracing apps to delete personal data after the crisis has subsided.**

We have seen that the public will support emergency or extreme measures that require curtailment of liberty or agency, or the increase of surveillance, if it is clearly justified for public good and solidarity. However there will need to be cast iron 'sunset' clauses to dismantle any data tracking and surveillance architecture as definitively and transparently as lifting restrictions on physical movement.

> **Government must lay out in primary legislation stipulating when, why and under what conditions individuals are required to be tested for and disclose their immunity status, and preventing private and public actors from requesting or requiring disclosure of immunity status outside of defined circumstances.**

This rapid evidence review begins with an introduction (Chapter 1) and exploration of policymaking during crises (Chapter 2) before moving on to discuss digital contact tracing (Chapter 3), symptom tracking apps (Chapter 4) and immunity certification (Chapter 5) in turn. The review brings forward core design options for the various technologies under consideration, discusses their technical limitations, canvasses the social and technical risks (and measures for mitigating those risks) and – where appropriate – explores possible accompanying policy measures.

The Ada Lovelace Institute has produced this evidence review swiftly with input from a range of experts in technology, law, philosophy, sociology and bioethics. Due to the timescales we have focused on England, but recognise that some of the issues are devolved matters and that the UK's devolved administrations will need to adapt some recommendations to meet their needs and responsibilities. However, the science, evidence and policy is very fast-moving, and any 'final' determination or conclusion advanced here would likely be outdated within days. As such, this rapid evidence review is an attempt to open up, rather than close down, an informed and public dialogue on the technical considerations and societal implications of the use of technology to transition from the crisis.

Findings and recommendations

Cross-cutting findings from this brief

Finding: Data-driven technologies may be effective tools in any transition strategy, but they are not a replacement for policy. Technologies must form part of holistic public health surveillance strategies and other pandemic response initiatives; without supporting evidence, they can and should not replace other proven methods.

Recommendation: Government must be transparent about the technical solutions under development. Technological solutions must complement, rather than replace, ongoing public health surveillance and pandemic response initiatives. They must be grounded in a comprehensive strategy for the UK's transition out of the crisis, for which Government should develop, publish and invite public scrutiny.

Finding: Effective policy interventions using technology take account of the social dimension of technology and its societal impact, are designed with the input and involvement of people across society, and are monitored and evaluated to assess their social impact on individuals and communities.

Recommendation: Government must broaden the range of actors involved in decision making around the COVID-19 crisis beyond scientific advisory bodies. An independent Group of Advisors on Technology in Emergencies (GATE) should be established to stand alongside the Scientific Advisory Group for Emergencies (SAGE), with a remit to examine the evidence base for technical interventions during the crisis, make recommendations for their deployment and oversee their impact. The Group of Advisors should be diverse and representative, and include experts in data and technology, the social sciences and humanities, and representatives of vulnerable groups, civil society and local authorities. Its deliberations and findings should be made public.

Finding: There is a real risk that the expansion of state intrusion into individuals' lives that occurs during emergencies endures beyond the originating crisis. Technical and legal infrastructure built during this pandemic may be difficult to dismantle once it is over unless proper safeguards are in place. The technology sector may bring cutting-edge innovation to solve difficult problems, but a democratic deficit emerges when private sector providers (alone or in partnership with the public sector) are deputised to implement public health policy during times of crisis.

Recommendation: Legal and technical sunset clauses must be built into the design of new powers and technologies. Government must provide advance primary legislation regulating the processing of data by both public and private sector actors in the use of technology to transition from the crisis. Government must encourage privacy-by-design in technical implementations and must choose privacy-preserving protocols to underscore technical measures.[2]

Finding: Effective deployment of technology to support the transition from the crisis will be dependent on widespread public trust and confidence in those interventions.

Recommendation: Government must be transparent about the technical measures under consideration in advance of their deployment. Technical interventions should not be deployed until the Group of Advisors on Technology in Emergencies has examined the evidence base for their use, assessed their likely impact, and recommended their deployment. Open debate and scrutiny must be encouraged, to increase trust and raise public awareness of the complexity of the issues.

Finding: As we move into the transition phase, the government should be thinking about how decision making at pace can be underscored with real-time scrutiny, evaluation and independent oversight.

Recommendation: An independent oversight mechanism should be established to lead scrutiny of the Government's policy formulation and decision making in real-time during the crisis. There is a real-time scrutiny initiative underway in Scotland, where the Scottish Police have appointed John Scott QC to lead scrutiny of how the police are using their powers.[3] This type of model could be applied in other domains, and may be particularly critical to bring accountability and oversight to the use of data and technology to support transition measures.

2 Information Commissioner's Office. Data protection by design and default. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/ [Accessed 17.4.2020]

3 Police Scotland. (2020). Human rights lawyer to lead scrutiny of emergency police powers. *Scotland.police.uk*. Available from: https://www.scotland.police.uk/whats-happening/news/2020/april/human-rights-lawyer-to-lead-independent-scrutiny-of-coronavirus-emergency-police-powers [Accessed 16.4.2020].

Technology-specific findings

Digital contact tracing

Finding: There is currently insufficient evidence to support the use of digital contact tracing as an effective technology to support the pandemic response. The technical limitations, barriers to effective deployment and social impacts demand more consideration before digital contact tracing is deployed.

Recommendation: Government must establish an independent Group of Advisors on Technology in Emergencies to oversee the development and testing of any prospective digital contact tracing app. The Group of Advisors should be charged with adjudicating when a digital contact tracing app is ready for deployment, taking into consideration:

- Evidence establishing the need for digital contact tracing to support manual contact tracing;
- The widespread availability of coronavirus testing for the general population;
- The potential for the app to achieve wide and consistent use among more than 60% of the population;
- A comprehensive understanding of the data architecture underpinning the app.

The remit of the Group of Advisors must include the ability to stipulate:

- The parameters against which the risk-scoring algorithm integrated into the digital contact tracing app detects and scores contacts;
- What technical features a digital contact tracing app should have in order to render the most useful data;
- What design features a digital contact tracing app should have in order to make it accessible and ensure compliance with its instructions
- Privacy-preserving measures that the digital contact tracing app should integrate.

Finding: If a digital contact tracing app is approved for deployment, it will only be effective if used as a tool to supplement and assist manual contact tracing (performed by medical professionals on the basis of interviews with patients) and if based on confirmed diagnostic tests for the virus.

Recommendation: Resources must not be diverted from manual contact tracing or diagnostic testing to technology development. The deployment of a digital contact tracing app should be delayed until system capacity for testing and manual contact tracing is increased sufficiently to meet an increase in demand caused by the roll-out of the app. Testing and manual contact tracing capacity must be sufficient to cover those segments of the population who are digitally excluded because of their age, disability, vulnerability, device ownership or digital literacy.

Finding: The effectiveness of a digital contact tracing app will be contingent on widespread public trust and confidence, which must translate into broad adoption of the app.

Recommendation: In order to increase public trust and confidence, and guard against abuse and scope creep, Government should advance primary legislation to:

- Set out the limited purposes for data processing;
- Limit who has access to data and for what purpose;
- Require the deletion of data after specified periods, as well as exemptions from deletion of anonymised data for the use in research;
- Require the performance, publication and approval by the Information Commissioner's Office of a data protection impact assessment for all technical measures to support the crisis;
- Establish a power for the Information Commissioner's Office to develop a Code of Practice pertaining to the processing of data within the context of the crisis.

Legislation should also contain safeguards making uses of data in contravention of regulation unlawful. Such uses would include:

- Use as evidence in the adjudication or imposition of civil or criminal sanctions;
- Use in proceedings or adjudications relating to visa or immigration status or rights;
- Use in family or child proceedings;
- Use in any other types of legal proceedings;
- Use to support any actions for denial of welfare or other public or social benefits;
- The sharing of data with employers or insurers without the freely given consent of the individual;
- The reliance on data by an employer to terminate or alter the existing conditions of employment or service;
- The use to discriminate in a way that would be illegal under the Equality Act 2010.

Finding: Given the lack of evidence as to the effectiveness of digital contact tracing, there is no basis to conclude that a mandatory requirement to install a digital contact tracing app would be necessary or proportionate. From a pragmatic standpoint, mandating use of a digital contact tracing app is unlikely to be effective, enforceable or enjoy public support.

Recommendation: If the Group of Advisors recommends the deployment of a digital contact tracing app, it should consider what steps the Government could take to increase voluntary public adoption of the app, through incentives or automatic app updates pushed to users' devices.

Symptom tracking

Finding: Of the three technologies considered in this review, symptom tracking raises the fewest risks and concerns, but also has the most limitations in terms of data quality, coverage and accuracy.

Recommendation: Government should support and foster public trust in symptom tracking efforts by strengthening the governance landscape in which they are being deployed. Government should advance primary legislation to:

- Set out the limited purposes for data processing;
- Limit who has access to data and for what purpose;
- Require the deletion of data after specified periods, as well as exemptions from deletion of anonymised data for use in research;
- Require the performance, publication and approval by the Information Commissioner's Office of a data protection impact assessment for all technical measures to support the crisis;
- Establish a power for the Information Commissioner's Office to develop a Code of Practice pertaining to the processing of data within the context of the crisis.

Legislation should also contain safeguards making uses of data in contravention of regulation unlawful. Such uses would include:

- Use as evidence in the adjudication or imposition of civil or criminal sanctions;
- Use in proceedings or adjudications relating to visa or immigration status or rights;
- Use in family or child proceedings;
- Use in any other types of legal proceedings;
- Use to support any actions for denial of welfare or other public or social benefits;
- The sharing of data with employers or insurers without the freely given consent of the individual;
- The reliance on data by an employer to terminate or alter the existing conditions of employment or service;
- The use to discriminate in a way that would be illegal under the Equality Act 2010.

Immunity certification

Finding: There is broad agreement that widespread testing is the only route through which the UK can exit the coronavirus crisis. Immunity testing is likely to be a key part of this strategy. However, there does not yet seem to be a robust scientific means of testing immunity. As such, there is no credible basis for establishing a comprehensive regime of immunity certification at this time.

Recommendation: Until a robust and credible means of immunity testing is developed, Government should focus on developing a comprehensive strategy to establish how immunity testing will be conducted, how immunity will be certified, and how immunity certification will be integrated into policy and processes including those pertaining to travel, movement, work and schooling. The strategy should be made public and open to public scrutiny.

Finding: The establishment of a regime for immunity certification will have deep societal implications. It may lead to arbitrary and unfair restrictions on individuals' access to transport, services, employment, movement and other rights and freedoms on the basis of their immunity status. Discrimination and stigmatisation may become commonplace if immunity becomes an element of identity as we transition from the crisis. The public will need to trust and support any government strategy that centres on immunity certification.

Recommendation: Government strategy must clearly define the role that immunity certification will play during transition and beyond the crisis. It must be clear to the public what values are being prioritised and traded-off in a transition strategy that centres on immunity certification.

Government should advance primary legislation specifying when, why and under what conditions individuals are required to be tested for and disclose their immunity status, and preventing private and public actors from requesting or requiring disclosure of immunity status outside of defined circumstances. Parliament must ensure such legislation is subject to robust and expert debate and scrutiny.

Finding: Should an immunity certification regime be determined necessary, a secure digital system based on open standards may be an effective way of maximising benefits while minimising fraud and abuse. However, it would need to be bolstered by non-digital methods in order to account for digital exclusion and prevent further harm to vulnerable groups.

Recommendation: Government must establish an independent Group of Advisors on Technology in Emergencies to oversee the development and testing of any prospective digital immunity certification system. The Group of Advisors should be charged with stipulating privacy-preserving measures that the system should integrate, and measures for ensuring vulnerable groups are not excluded from the operation of the system.

1. Introduction

The first pandemic of the algorithmic age

For the first time in history, we are equipped with technological tools that can assist in every aspect of crisis response: from vaccine development and the rapid production and deployment of PPE, to remote working and virus diagnosis. Data-driven technologies can help to save lives during the present crisis.

But they may also expose people to new risks. Inaccurate, irresponsible or imprecise use of data or technology can undermine public health strategies, exacerbate the spread of the pandemic or erode public trust and confidence in authority and government. Bad use of data can be counterproductive – it can obscure truths, hide abuses of power, and stigmatise or disadvantage groups already suffering from health inequalities. Any diversion of resources from existing public health surveillance initiatives to technology development may undermine the pandemic response.

As the growth in the number of cases of the virus slows and the capacity of the healthcare system to handle new cases increases, governments will be looking to transition to a new phase of disease control, where countries try to live with the virus while research continues into both a vaccine and therapeutic measures that may reduce its fatality. This phase is expected to focus on trying to relax movement restrictions while monitoring for, and clamping down on, new outbreaks of the virus. This will require a new set of policies to be implemented.

Governments around the world are beginning to look to data-driven technologies as a means of giving effect to these policies. Three of the interlocking data-driven interventions being deployed or considered are symptom tracking applications, digital contact tracing applications, and immunity certificates.[4] All three provide potential means of identifying instances of the virus in individuals and communities, in order to facilitate research and public health interventions.

Development of symptom tracking and digital contact tracing apps in the UK has occurred in an ad hoc manner to date. Immunity certificates are, according to the Health Minister Matt Hancock, under consideration.[5] No policy proposal or strategy has yet been advanced outlining how these technologies are situated within the Government's broader transition strategy.

4 There are many others that are outside the purview of this briefing, including the use of technology to monitor and mitigate the spread of misinformation on social media platforms, such as: Ofcom. (2020). Covid-19 news and information: consumption and attitudes. *Ofcom.com*. Available from https://www.ofcom.org.uk/research-and-data/tv-radio-and-on-demand/news-media/coronavirus-news-consumption-attitudes-behaviour [Accessed 16.4.20].

5 Bartlett, N. (2020). Government plans 'immunity passports' for people to escape coronavirus lockdown. *The Mirror* [Online]. Available from: https://www.mirror.co.uk/news/politics/government-looking-immunity-passports-people-21803546 [Accessed 16.4.2020].

More than at any other time, technologies deployed during national and international crises must enjoy public trust and support in order to fulfill their potential usefulness. That is particularly the case when the widespread uptake of technologies is critical to their success. In order to ensure that data-driven interventions in the present crisis are designed, deployed and governed in a way that is consistent with public expectations, respectful of human rights and in the public interest, the legal, ethical and technological questions they raise must be considered in advance.

About this review

This rapid evidence review explores the legal, societal and technological impacts of certain data-driven technologies, in order to understand their ethics and their impact, with a particular eye on the societal impact of technologies on inequality and vulnerable groups. This review focuses on three technologies in particular:

Digital contact tracing applications: a computer program that can be installed on a user's personal device, which determines when a person has come into contact with a person or number of persons infected with COVID-19, and subsequently notifies either the person or a public health authority to provide guidance or instructions. The purpose of digital contact tracing applications is to support efforts to control the spread of the disease and better target isolation measures.

Symptom tracking applications: a computer program, either installed on a user's personal device or accessed via a website, which asks users to submit details of their symptoms, and optionally, other data such as name, geographical location, GPS location, IP address, social media credentials, age, gender, occupation, medical history, household information, etc. The purpose of symptom tracking applications is to increase understanding of the disease, support research and understand its spread.

Digital immunity certificates: a digital token or other form of authentication that a person has been infected with coronavirus disease in the past and is now presumed to have a form of immunity for a period of time. The purpose of digital immunity certificates is to enable people at no risk of further infection of the disease to return to work, care for the ill and begin to restore the capacity of social, economic and health systems.

This review is authored by the Ada Lovelace Institute, a research institute and deliberative body with a remit to ensure that data and AI works for people and society, and is informed by the input of more than twenty experts drawn from across a wide range of domains, including technology policy, human rights and data protection, public health and clinical medicine, behavioural science and information systems, philosophy, sociology and anthropology.

The Ada Lovelace Institute is an independent institution which seeks to ensure that the public interest is represented in debates around the use of technology. This review makes pragmatic recommendations on issues of data and technology to support well-informed policymaking in response to the crisis. It has been prepared in the context of a fast-moving crisis in which our understanding of the disease, our access to evidence about it and the impact of responsive measures, and government policy is changing rapidly.

It makes recommendations to Government and the NHS, Parliament and the public about how to ensure that data-driven interventions ameliorate, rather than exacerbate, the crisis.

2. Policymaking during crises

In times of crisis we need to pay more attention more than ever to how complex technological and societal uncertainties are democratically resolved, and what is lost or simplified – in the interests of expediency – in critical policymaking.

Decisions about technology made during the COVID-19 crisis occur against the background of recent rapid change in societal relationships with technology, existing public distrust of data handling by tech companies and governments, and unanswered questions about private-public partnerships that distribute risk and limit accountability.

In tackling COVID-19, what is being proposed is technology acting as an instrument of governance: a modern technological system being given the powers of a legal constitution to order and govern society without the centuries of legal and political theory that underpin prior consent in those institutions. In the absence of these accepted conventions, there are scant tried-and-tested mechanisms for controlling risk, mitigating against inequality and incorporating human values.

If these new technologies are permitted to operate for social good and serve collective not individual purposes in mitigating the effects of the virus, the need for responsibility for anticipating and safeguarding against the short- and long-term negative impacts of these technologies will be heightened. There is a real danger that the Government will provide a sense of democratic supervision while giving private-sector technology companies the freedom to determine what counts as public good, and that the consequences of these decisions will persist long beyond the crisis and the exit strategy.

Human rights and data protection

This rapid evidence review does not contain an analysis of the compliance of technical solutions with human rights or data protection law. However, it begins from the understanding that the principles contained within both frameworks are the foundational principles against which any Government policy, including technology adoption, must be measured. Any technology employed and implemented – whether by state or private actors – will also be measured against these principles.

At times of crisis, exceptional measures to curtail individual rights may become lawful, necessary and proportionate. For example, social isolation restrictions, unthinkable in ordinary times, may become permissible – and necessary – in exceptional ones.[6] Equally, the deployment of digital means to monitor and track the spread of a disease, if implemented proportionately and with appropriate safeguards, may meet the thresholds which make them legitimate under human rights law. To do so they will not only need to be grounded in a clear legal framework, but be strictly necessary to achieve a legitimate aim, such as the protection of public health, and be proportionate to that aim.

Assessments of necessity and proportionality will need to consider the effectiveness of the particular intervention in achieving the legitimate aim, and whether less intrusive measures could achieve that same aim. These are the essential questions asked by this review: are the technical solutions proposed feasible and effective, and will they add additional value to the crisis response?

Data protection principles echo and underscore this approach, and also demand contemplation of how mitigation measures may minimise infringements on individual data rights, including privacy, through principles such as purpose limitation (data should be collected for specified and explicit purpose and not used in another manner), data minimisation (only using the data needed to achieve a goal) and data protection by design.

Ethical values

Human rights and data protection may not provide us with sufficient tools to navigate the trade-offs that can be necessary during times of exceptional emergency. The balancing of privacy on the one hand, and the protection of other human rights, such as the right to life, on the other, may appear simple in the abstract, but developing policy and technology at pace which honours a legitimate balance is complex.

Solidarity implies acting in a way that is best for our societies, not only for us as individuals. Ethical values can help us navigate this.

However, emergencies do not provide ideal environments for ethics-based assessments. High levels of need and urgency, compounded by lack of strategic clarity and rapidly changing circumstances, make it particularly difficult.[7] This rapid evidence review is not an ethical analysis. The Ada Lovelace Institute intends to undertake such an analysis subsequent to the publication of this review.

In the meantime, we should acknowledge that methods to assess risk, success and failure will not be value-neutral, and that decisions will be value-laden. There may be unethical paths that can be taken, but there is not a single 'ethical' approach to recovery from this pandemic. Values and liberties will need to be weighed and traded-off, such as individual liberty and the public good; new contingencies to dignity and vulnerability; or agency and solidarity.

6 Tom Hickman QC, Emma Dixon and Rachel Jones, *Coronavirus and Civil Liberties in the UK*, 6 April 2020. Available from: https://coronavirus.blackstonechambers.com/coronavirus-and-civil-liberties-uk/

7 Nuffield Council on Bioethics. (2020). Research in global health emergencies: ethical issues. *Nuffieldbioethics.org*. Available from: https://www.nuffieldbioethics.org/publications/research-in-global-health-emergencies [Accessed 16.4.20].

This is a time of political leadership and accountability, when trade-offs and guidance principles need to be made explicit by decision makers, in particular, those that balance individual rights against public good.

Technology for transition – comparative experiences

In the transition phase it is expected that people will be able to move more freely where there are no outbreaks of the virus or if a test shows that an individual has a level of immunity.[8] During the transition phase, public health authorities will need to quickly identify and intervene to stop each new outbreak and save lives, while research will continue into a vaccine and therapeutic measures.

Other countries have already entered this next phase. Three that are frequently discussed are China, South Korea and Singapore. All three are using a mix of social and technical measures. There is currently no published, peer-reviewed, research which compares the effectiveness of these measures against public health objectives.

China, where this outbreak started, has started to relax lockdown measures in cities and is using technical measures as part of its efforts to reduce the chance of further outbreaks. People who are found to have the virus are quarantined. Two QR-enabled health status applications – the Alipay Health Code developed by Ant Financial, a sister company of Alibaba, and a rival application developed by TenCent – are being used by local authorities, employers, cafes and restaurants to inform movement and work restrictions.[9] The applications assign individuals a colour-coded health status that is used as part of measures to control where and when people can travel. The method by which the health status is determined has not been published, but it is believed it draws on location data, self-reported health data and national identity number, among other sources.[10] It is not clear how many mistakes are made or whether people can appeal their status.

8 Association of the British Pharmaceutical Industry. (2020). What is the life sciences sector doing to help increase COVID-19 testing? *Abpi.org.uk*. Available from: https://www.abpi.org.uk/medicine-discovery/covid-19/briefing-coronavirus-covid-19-testing/ [Accessed 16.4.20].

9 Mozur, P, Zhong, R, Krolik, A. (2020). In Coronavirus fight, China gives citizens a color code, with red flags . *New York Times* [Online]. Available from: https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html [Accessed 16.4.2020].

10 Lindberg, K, S, Hong, J. (2020). People in China need a green light from Alipay app to move around. *Japan Times* [Online]. Available from: https://www.japantimes.co.jp/news/2020/03/24/asia-pacific/china-green-light-alipay-app/#.XpFm0MhKg2w [Accessed 16.4.20].

South Korea has a program of testing (including drive-through testing), mask distribution, contact tracing and quarantine.[11] Law enforcement authorities check that these rules are being followed. Quarantined individuals are required to download a government app which monitors their location and is used to enforce quarantine, as well as connect them to health care workers.[12] Contact tracing is enhanced through the use of mobile phone location data, and the government broadcasts messages about infected individuals' movements.

Singapore's experience of the coronavirus crisis has been inverted when compared with other countries'. Social distancing measures mandated were, until early April, mild, and excluded any broad restrictions on movement. Instead, rigorous contact tracing by police and local authorities had been effective in stemming the spread of the virus. The use of CCTV footage, credit card records and the TraceTogether digital contact tracing app has also been deployed by Singaporean authorities to enhance contact tracing initiatives. There is as yet no research available on the impact of using the app or the extent to which it has made contact tracing more effective. In early April, social isolation measures were strengthened in Singapore, with strict fines and penalties levied on those who contravene them.

Taiwan could claim the lowest incidence per capita of COVID-19 infections as of mid-March 2020. The country acted quickly to shut borders, issue guidance to schools regarding disinfection, and centralise public health surveillance efforts. In terms of technical tools, temperature monitors already in place following the 2003 SARS outbreak along with widespread temperature-taking in office buildings, schools and homes has been supplemented by online symptom tracking using QR codes for travellers, mandatory quarantine and a rigorous regime of testing and contact tracing.

11 Cha, V. (2020). South Korea offers a lesson in best practices. *Foreign Affairs* [Online]. Available from: https://www.foreignaffairs.com/articles/united-states/2020-04-10/south-korea-offers-lesson-best-practices [Accessed 16.4.20].

12 Kim, M. (2020). South Korea is watching quarantined citizens with a smartphone app. *MIT Technology Review* [Online]. Available from: https://www.technologyreview.com/2020/03/06/905459/coronavirus-south-korea-smartphone-app-quarantine/ [Accessed 16.4.20].

3. Digital contact tracing

Chart 3
Overview of digital contact tracing

Public health surveillance during pandemics enables public health authorities to understand who is at risk of catching the disease, and put in place proportionate health measures to help people who may have caught the disease and reduce the chance of it spreading further.

Contact tracing is a standard method to help with this process. Typically this is performed manually by speaking with patients to identify anyone who has had close contact with them during the time they are considered to be infectious. Each of those people is located as soon as possible, and placed in isolation or quarantine.[13]

13 Phin, N. (2020). Coronavirus (COVID-19) Expert interview: What is contact tracing? *Gov.uk*. Available from: https://publichealthmatters.blog.gov.uk/2020/02/13/expert-interview-what-is-contact-tracing/ [Accessed 16.4.20].

In the UK contact tracing for COVID-19 was halted when the virus reached a level of sustained transmission across the country.[14] Some experts say that this was due to low testing and tracking capacity.[15] In a transition phase where the UK is trying to live with the virus while quelling outbreaks, contact tracing may need to be reinstated on a large scale. Digital means of conducting contact tracing are under consideration.

How does it work?

Digital contact tracing uses devices carried by people, for example a smartphone, as a proxy for people. It measures the proximity of those devices to each other and uses it as a proxy for contact between two or more people.[16] This data is analysed by a risk-scoring algorithm according to certain parameters (such as length of contact and number of contacts with persons reported to be infected with the virus, on the basis of either self-reported or verified testing data) to determine whether a user or public health authorities should be alerted about potential contact and what action should then be taken. It can be seen either as a replacement or a complement to manual tracing initiatives and can be connected with a testing strategy that identifies people who are infected.

On 12 April 2020, the UK Government confirmed it is developing a digital contact tracing app and that it will be testing the app during the week commencing 13 April 2020.[17]

Design options

There are a number of different approaches to digital contact tracing being proposed and implemented around the world. Each of them employs different designs, in different political, legal and social contexts.[18] The decision as to how a particular app is designed will take into account a number of medical, technical and societal factors such as testing and clinical healthcare capacity, manual contact tracing capabilities, availability of smartphones, sensitivity to privacy issues, or trust in government.

---

14 Gregory, A. (2020). UK defends strategy as WHO urges governments to test citizens as 'backbone' of coronavirus response: 'Test, test, test'. *The Independent* [Online]. Available from: https://www.independent.co.uk/news/health/coronavirus-test-world-health-organisation-uk-contact-tracing-chris-whitty-phe-a9405476.html [Accessed 16.4.20].

15 Tapper, J. (2020). Government plans 'immunity passports' for people to escape coronavirus lockdown. *The Guardian* [Online]. Available from: https://www.theguardian.com/world/2020/apr/04/recruit-volunteer-army-to-trace-coronavirus-contacts-now-urge-top-scientists [Accessed 16.4.20].

16 Ross Anderson of the Department of Computer Science and Technology at the University of Cambridge has written about some of the technical and social challenges of different approaches to contact tracing at: https://www.lightbluetouchpaper.org/2020/04/12/contact-tracing-in-the-real-world [Accessed 16.4.20].

17 Kelion, L. (2020). UK confirms plan for its own contact tracing app. *BBC News* [Online]. Available from: https://www.bbc.co.uk/news/technology-52263244 [Accessed 16.4.20].

18 According to Linklaters, as of 15 April 2020 28 countries had launched official contact tracing apps (13 of which were in Asia and 11 in Europe), with a further 11 countries known to be developing them. Available from: https://www.linklaters.com/en/about-us/news-and-deals/deals/2020/april/28-countries-race-to-launch-official-covid-19-tracking-apps-to-reduce-the-spread-of-the-virus [Accessed 16.04.20].

Mandatory or voluntary

Singapore's TraceTogether service is voluntary, it is reported that about 13% of the population are using it.[19] The UK Government has signalled that the NHSX app will also be voluntary. In Israel, emergency legislation permits government officials to conduct digital contact tracing on people with confirmed infections using existing mobile data records.[20] A similar model is being used in China where, as with other Chinese digital public health initiatives, the details of the implementation can be expected to vary by province.

Infection reporting

Infection could be reported to a digital contact tracing app in a number of ways: an individual could self-report infection to an app; they could self-report and upload confirmation from a medical professional or an approved test; a medical professional or testing service could notify the digital contact tracing service that their patient is infected, or public health authorities could upload a list of patients that are infected. Reportedly, the NHS app will provide a different type of alert based on whether the infection report is self-reported by an individual or made by a medical professional.

Protocol and application

Some initiatives are focused on developing protocols on which digital contact tracing apps can be built. Singapore's BlueTrace uses Bluetooth signals to capture proximity between devices. The data collected by the app is then stored centrally for analysis.

Newer protocols are more focused on privacy-preserving ways to share information captured by Bluetooth signals. These initiatives include Google and Apple's, the European PEPP-PT initiative, the multi-institution DP-3T proposal and MIT's Safe Paths.[21] These protocols allow app developers, with epidemiologists, to tune risk-scoring algorithm parameters such as proximity and duration before a contact is recorded. The parameters for the risk scoring algorithm are generated centrally before being distributed to the apps on the phones. The parameters will need to be adapted over time as more is learned about how to make digital contact tracing effective while protecting against risks. Systems such as DP-3T allow anonymous data to be received by epidemiologists to inform these parameters and improve them over time.

Other countries have started building apps in parallel with these protocols. These apps may use variants of the protocols and will influence the design of them. The UK's NHS contact tracing app is one of these initiatives. This app started development before the protocols were published and it remains to be seen which, if any, of the protocols it will use when it is deployed or if it will need to adopt a protocol after it is launched.

---

19 The Economist. (2020). Countries are using apps and data networks to keep tabs on the pandemic. *The Economist* [Online]. Available from: https://www.economist.com/briefing/2020/03/26/countries-are-using-apps-and-data-networks-to-keep-tabs-on-the-pandemic [Accessed 16.04.20].

20 Lomas, N. (2020). Israel passes emergency law to use mobile data for COVID-19 contact tracing. *TechCrunch* [Online]. Available from: https://techcrunch.com/2020/03/18/israel-passes-emergency-law-to-use-mobile-data-for-covid-19-contact-tracing/ [Accessed 16.4.20].

21 BlueTrace Protocol. (2020). Available from: https://bluetrace.io/ Pan-European Privacy-Preserving Proximity Tracing (2020). Available from: https://www.pepp-pt.org Decentralized Privacy-Preserving Proximity Tracing (2020). Available from: https://github.com/DP-3T MIT Media Lab. (2020). Safe Paths: A privacy-first approach to contact tracing. *News.mit.edu*. Available from: http://news.mit.edu/2020/safe-paths-privacy-first-approach-contact-tracing-0410 [All accessed 16.4.20].

The protocol choice influences other aspects. For example, Singapore's TraceTogether application requires iPhone users to keep their phones unlocked in their pocket, with screens on and the app foregrounded, for it to work. This has reportedly led to low adoption, because of lack of use, and the privacy, security and identity theft risks of having an unlocked phone which can be stolen. Apple has indicated that from early May 2020, this will not be necessary, but only for apps which do the matching of identifiers privately on the device, rather than on a central server as Singapore's does.

In the future, it will likely be important to consider how apps interoperate to allow 'roaming' across borders, such that individuals can still receive alerts when they have been near someone who later tested positive in a different country.

Data collected

Some Bluetooth-based digital contact tracing apps only collect an anonymised, constantly changing ID created by other devices running an app based on the same protocol. The different protocols use differing methods to create these IDs based on a balance of public health and privacy needs.

Apps can also collect data such as location information or how the user interacts with the app. This can happen regardless of the protocol and form part of the broader design of the app, for example as well as an app using a Bluetooth protocol it could also collect GPS data. Such data can be used to inform the information an app provides to the user when they are alerted to a contact, such as the location of the nearest testing clinic, without that location data ever being transmitted.

Other digital contact tracing services rely on data collected as people interact with other parts of a national data infrastructure; for example South Korea collects telecoms data and credit card information.

Data access

A protocol and app can be designed to use decentralised models with most data collected by an app and stored on the smartphone. In this model a user who is infected gives consent for information about the smartphones that they may have been in contact with to be uploaded to a central server. Other smartphones regularly download this list of IDs that are reported to be infected and notify their user if this information identifies that they may have been in contact with an infected person.

Other protocols and services use more centralised models with information about digital contacts – whether collected from devices, telecoms networks, credit card data or other sources – stored and analysed in a central location.

Contact alerting

When a digital contact tracing app determines that its user may have been in contact with someone who is infected then the user will be notified. Some digital contact tracing apps, for example those in China and South Korea, also report the contact or the individual user to public health authorities to help to track new outbreaks or monitor and enforce self-isolation or quarantine for infected individuals.

Actions

In line with a country's medical advice and practices a user can be notified to check their symptoms, report to a testing centre, or to quarantine themselves for a period of time. In Singapore a medical professional helps a user to interpret the notification and decide what action to take. Public health authorities are expected to need flexibility in the action that the app will recommend as they learn how to make digital contact tracing an effective part of a national public health strategy.

App	Mandatory or voluntary	Protocol	Data collected	Data access	Infection reporting	Contact alerting	Actions
NHS app (in development)	Voluntary	To be determined	IDs created by nearby phones	User and public health authorities	Self-reported and by medical professionals	To user and medical professionals	Quarantine if infection reported by medical health professionals
Singapore Trace Together (live)	Voluntary	Bluetrace	IDs created by nearby phones	User only	Medical professionals	To user and medical professionals	Decided by medical professional
South Korea (live)	Mandatory	Not applicable	Citizen location information, credit card data	User and public health authorities	Self-reported and by medical professionals	To user and medical professionals	Quarantine
Taiwan (in development)	Mandatory	Not applicable	Citizen location information, credit card data	User and public health authorities	Self-reported and by medical professionals	To user and medical professionals	Quarantine
Germany, France, Estonia and other EU countries (in development)	Voluntary	PEPP-PT	IDs created by nearby phones	To be determined	To be determined	To be determined	To be determined
Israel (live)	Mandatory	Not applicable	Citizen location information, credit card data	User and public health authorities	Self-reported and by medical professionals	To user and medical professionals	Quarantine

Table 1
Comparison of proposed international digital contact tracing apps

There are a number of technical, institutional and practical barriers to the effective deployment of digital contact tracing.

Technical limitations

The technical limitations to digital contact tracing render it a poor substitute for manual contact tracing, and mean that digital contact tracing must complement, rather than replace, manual contact tracing.

1. Imprecision in detecting 'contact'

COVID-19 is primarily transmitted from infected (both asymptomatic and symptomatic) people to others who are in close contact through respiratory droplets, by direct contact with infected persons, or by contact with contaminated objects and surfaces.[22] Because digital contact tracing uses proximity of digital devices as a proxy for contact, it needs to use measurable vectors, such as distance and time, to ascertain when a contact incident occurs, but these will necessarily be imprecise, and could lead to high numbers of false positives and false negatives.[23] Digital contact tracing will be less able to control for variables such as ventilation, direction of wind or environment, factors that are normally central to manual contact tracing efforts.

2. Imprecision in detecting distance

Four technical mechanisms exist for detecting distance: GPS, mobile network signals, WiFi or Bluetooth signals. Each has their limitations in detecting distance. GPS works best outside, so will have more imprecision when determining contact between people inside of buildings or underground rail networks.

Mobile network signals have similar limitations. Unlike GPS their level of precision will also vary based on the number of mobile masts in a particular area. This tends to make them less precise in rural areas. WiFi-based tracking would determine when two people are both on the same WiFi network, but would not necessarily ascertain when they are in close enough proximity for contact to be usefully established. Bluetooth works indoors and outdoors, has existing research that describes methods for estimating difference between two devices due its use in commercial activities such as marketing, but Bluetooth capability is not ubiquitously available on all devices.[24]

3. Vulnerability to fraud and abuse

As with any technology, digital contact tracing will be vulnerable to all forms of fraud and abuse – from people using multiple devices, false reports of infection, to denial of service attacks by adversarial actors.

---

22 World Health Organisation. (2020). Coronavirus disease 2019 (COVID-19) Situation Report – 73. *Who.int*. Available from: https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200402-sitrep-73-covid-19.pdf?sfvrsn=5ae25bc7_6 [Accessed 16.4.20].

23 The Intelligence Podcast. (2020). An app for that: Covid surveillance. *The Economist* [Online]. Available from: https://podfollow.com/1449631195/episode/8f7e261398cd1ff2950c8124f47a2d2a14294a21/view [Accessed 16.4.20].

24 Landau, S. (2020). Location surveillance to counter COVID-19: efficacy is what matters. *Lawfare* [Online]. Available from: https://www.lawfareblog.com/location-surveillance-counter-covid-19-efficacy-what-matters [Accessed 16.4.20]

The many technical limitations of digital contact tracing led Singapore's product lead for the TraceTogether app, Jason Bay, to conclude:

> 'The experience of Singapore's contact tracers suggest that contact tracing should remain a human-fronted process. Contact tracing involves an intensive sequence of difficult and anxiety-laden conversations, and it is the role of a contact tracer to explain how a close contact might have been exposed — while respecting patient privacy — and provide assurance and guidance on next steps.
>
> 'A human-out-of-the-loop system will certainly yield better results than having no system at all, but where a competent human-in-the-loop system with sufficient capacity exists, we caution against an over-reliance on technology.'[25]

However, digital epidemiologists Marcel Salathé and Ciro Cattuto note that the contagious nature of COVID-19 also creates an important role for digital contact tracing compared to traditional contact tracing:

> 'Normally, contact tracing is done through interviews. But interviews alone can be problematic because i) they are slow, ii) they are difficult to scale because of resource requirements (e.g., required human effort), and iii) a "contact" in the case of a respiratory disease may be anyone who has been in close-range physical proximity (i.e. 2 meters) for some time (i.e. a few minutes). This can of course include strangers which one would never be able to recall in a traditional interview. Digital proximity tracing through apps could help solve these problems.'[26]

25 Bay, J. (2020). Automated contact tracing is not a coronavirus panacea. *Government Digital Service blog*. Available from: https://blog.gds-gov.tech/automated-contact-tracing-is-not-a-coronavirus-panacea-57fb3ce61d98 [Accessed 16.4.20].

26 Salathé, M, Cattuto, C. (2020). COVID19 Response – What data is necessary for digital proximity. *Digital Epidemiology Lab Occasional Paper*. Available from: https://github.com/digitalepidemiologylab/COVID-documents/blob/master/COVID19%20Response%20-%20What%20Data%20Is%20Necessary%20For%20Digital%20Proximity%20Tracing.pdf [Accessed 16.4.20].

Barriers to effective deployment

1. Effectiveness needs to be established

At the time of writing there is no public study into the effectiveness of digital contact tracing, the different techniques that countries are employing, and how digital contact tracing forms part of a wider pandemic response strategy. Every country is selecting an approach that they think fits their social context and technical capabilities. As studies are published and more deployments are performed, individual deployments may need to adapt to this new information. This will require each country to measure and report on effectiveness, while retaining the ability to change direction.

2. It relies on high levels of accuracy and ubiquity

In order to avoid the limitations of symptom tracking, digital contact tracing would need to be premised on accurate and verified information about infection rates. That is, if digital contact tracing were to provide a higher quality of data than self-reported symptom tracking, it would need to be reliant on accurate diagnostic testing as to acquisition of the virus. Even if diagnostic tests undertaken in UK hospitals have a high degree of accuracy, they are currently only being carried out on the most severe cases, or on key workers. Fewer than 300,000 tests have been carried out in the UK to date.[27]

Beyond accurate testing, effective digital contact tracing relies on a high level of uptake by the population. A mathematical model and paper,[28] developed by a research cohort led by Oxford University's Nuffield Department of Medicine for NHSX, found that a digital contact tracing app could be effective in suppressing the epidemic if approximately 60% of the population used the app. The research assumes 100% compliance with self-isolation instructions delivered by the app (with 2% drop out each day). Researchers estimate lower numbers of users could still have a positive effect on the spread of the disease.

A figure of 60% of the population is equivalent to 80% of people who own smartphones. Ofcom figures show that 22% of UK adults do not have a smartphone, rising to 45% of adults over 55, and that figures on device ownership for young children vary.[29] The published work by the Oxford group includes an online citizen survey of 1,055 UK adults in which '74% of respondents said they would definitely or probably install the app'.[30]

3. Public trust and confidence

Digital contact tracing will only become an effective tool for transitioning out of the crisis if it enjoys public buy-in. Efforts to increase the ubiquity of digital contact tracing apps, including through mandating their use, could have the opposite effect, undermining public trust and confidence in government and even provoking civil disobedience. The public could refuse to comply and choose sanctions over participation, which would undermine the effectiveness of the endeavour.

---

27 Schraer, R. (2020). Coronavirus: Testing and why it matters. *BBC News* [Online]. Available from: https://www.bbc.co.uk/news/health-51943612 [Accessed 16.4.20].

28 Robert Hinch et. al., Effective configurations of a digital contact tracing app: A report to NHSX, 14 April 2020 (version 2). Available from: https://github.com/BDI-pathogens/covid-19_instant_tracing/blob/master/Report%20-%20Effective%20Configurations%20of%20a%20Digital%20Contact%20Tracing%20App.pdf

29 Ofcom. (2019). Online nation: 2019 report. *Ofcom*. Available from: https://www.ofcom.org.uk/__data/assets/pdf_file/0025/149146/online-nation-report.pdf [Accessed 16.4.20].

30 Nonsenzo, D. et al. (2020). User acceptance of mobile contact tracing app. *Medsci.ox.ac.uk*. Available from: https://045.medsci.ox.ac.uk/user-acceptance [Accessed 16.4.20].

People might fear that government agencies will use digital contact tracing apps to track their movements and who they associate with, in order to inform decisions about potential illegal behaviour or immigration proceedings. (Significantly, a service might incorrectly flag someone as a contact if a person comes into contact with them in another way, such as sitting next to them on a bus.) This is particularly significant given the effect on public trust in some communities following incidents such as the Metropolitan Police Gangs Matrix, Windrush deportations and ongoing anti-terrorism activity such as the Prevent programme.[31] An untrusted digital contact tracing service could lead to a disproportionate effect on health outcomes and lead to further outbreaks of the virus which might concentrate in particular groups but could then spread to the wider population. In a pandemic it is vital for societies to find ways to reach and protect the health of everyone.

To cater for these variations there will need to be a level of agility in how digital contact tracing is implemented, ongoing user research into how the service is perceived by citizens, active solicitation of thoughts from vulnerable groups, action on all of these insights, and ongoing monitoring of any service's effectiveness in delivering the desired public health outcomes.

In addition, public acquiescence and confidence could be achieved through clear Government commitment to:

- **Privacy-by-design**: As the DP-3T proposal evidences, decentralised privacy-preserving digital contact tracing is feasible through technical measures.[32] Ensuring technical protection of individual privacy is a central means (though not a sufficient one) to shore up public confidence in digital contact tracing.
- **Robust regulation and oversight**: Neither existing legislation or the Coronavirus Act cover all of these risks. Primary legislation will need to be advanced in order to establish the legal basis for data processing, prevent the reuse of data processed through the app, and establish an oversight and redress mechanism to guard against abuse.
- **Time-limitation**: Legislation will need to specify a time-limited period during which digital contact tracing is mandated and restrict renewal of the period to a maximum number of subsequent periods.
- **Purpose limitation**: Legislation will need to specify the purposes for which data collected by digital contact tracing apps can be used.
- **Clear guidance on application and enforcement**: National guidance on the enforcement and use of digital contact tracing will need to be developed and disseminated.
- **Transparency**: Designs, research and source code for digital contact tracing and data about its use and effectiveness in reducing the spread of the virus will need to be made public, in order to enable public scrutiny of the effectiveness of the approach.

31 Amnesty International. (2018). What is the Gangs Matrix? *Amnesty.org.uk*. Available from: https://www.amnesty.org.uk/london-trident-gangs-matrix-metropolitan-police Williams, W. (2018). Windrush lessons learned review. *Gov.uk* [Online]. Available from: https://www.gov.uk/government/publications/windrush-lessons-learned-review Bowcott, O. (2019). Lord Carlile removed from Prevent review after legal challenge. *The Guardian* [Online]. Available from: https://www.theguardian.com/uk-news/2019/dec/19/lord-carlile-prevent-review-legal-challenge [All accessed 16.4.20].

32 Decentralized privacy-preserving proximity tracing. (2020). Available from: https://github.com/DP-3T [Accessed 16.04.20].

4. Potentially harmful behavioural impacts

Effective deployment of digital contact tracing apps requires widespread uptake. In Singapore, where more than one million people have downloaded the TraceTogether app, authorities have recognised that the number is nothing close to what is needed to render the app effective – 75% of the country's population, they estimate.[33] Estimates like this are based on mathematical models and carry uncertainty, particularly as the effectiveness of the current digital contact tracing approaches have not yet been measured.

The value of an ineffective digital contact tracing app is questionable – it may put individuals at more risk by giving them incomplete information, and a false sense of security (or insecurity). Individuals who are the most vulnerable to the virus, and arguably who would benefit most from digital contact tracing apps, are those least likely to own a smartphone or have the digital literacy skills to use such an app. Those who suffer from health inequalities, including inequalities linked to place and socio-economic status, are also more likely to be on the wrong side of the digital divide.[34]

Measures to address some of the technical, institutional and practical barriers raised above could be taken, including increasing the ubiquity of deployment through automatic updates pushed to users' mobile phones, laws mandating deployment or making lockdown reduction conditional on aggregate national use of a digital contact tracing app. Those without smartphones or Bluetooth devices could be provided with Bluetooth tokens as part of the initiative.

However, even assuming digital contact tracing apps could be rendered effective through near-ubiquitous deployment, it will be critical to think about how they convey information to users in a way that has the intended effects on behaviour. It is unlikely that instructions delivered via an app to self-isolate or quarantine will have the same effectiveness as similar messages delivered by a human contact tracer or public health official. This is particularly the case if the data in the app is based on self-reporting, rather than verified testing data. Compliance with instructions to self-isolate or quarantine, provided by the app, could also be mandated by regulation and enforced by law enforcement officials. However, the limitations of digital contact tracing mean that it is unlikely to be considered sufficiently necessary and proportionate to justify the infringement on human rights occasioned by enforced quarantine.

Moreover, enforcement of any mandatory requirement to participate in digital contact tracing would likely fall on police services, which are already operating in incredibly difficult circumstances to police compliance with social distancing measures. In contexts in which the capacity for policing of compliance universally and equitably is diminished, there is a real risk of disproportionate enforcement.

33 Chong, C. (2020). About 1 million people have downloaded TraceTogether app, but more need to do so for it to be effective: Lawrence Wong. *Straits Times* [Online]. Available from: https://www.straitstimes.com/singapore/about-one-million-people-have-downloaded-the-tracetogether-app-but-more-need-to-do-so-for [Accessed 16.4.20].

34 Office for National Statistics. (2019). Exploring the UK's digital divide. *Ons.gov.uk* [Online]. Available from: https://www.ons.gov.uk/releases/exploringtheuksdigitaldivide [Accessed 16.4.20].

Social considerations need to be built in

Government policymaking will need to consider the second order impacts of widespread deployment of digital contact tracing. These include:

1. Potential exclusion of vulnerable groups and exacerbation of health inequalities

The Good Things Foundation Digital Nation report shows information about people who have low digital skills and the correlations with poor health, old age and low income.[35] As well as prompts within any digital contact tracing app, some level of continued manual contact tracing will be required in order to ensure vulnerable groups are not excluded from digital contact tracing or that people who already suffer from health inequalities do not fall through the gap. Ensuring a digital contact tracing app is accessible for people with disabilities, neurodiverse people and others who might have difficulty with inaccessible digital technologies will also be key to ensuring that digital contact tracing doesn't exacerbate inequalities. Equally, individuals from black and ethnic minority backgrounds with historic experiences of discrimination and police surveillance are less likely to adopt and benefit from digital contact tracing apps, even as they are more likely to suffer from adverse health outcomes.

2. Direct and indirect societal and financial implications

Successful digital contact tracing will mean that, even as society and the economy opens up to begin an exit from the crisis, individuals will continue self-isolating or quarantining. Guidance to employers, public benefits and support, and alterations to the health service will all be necessary to ensure a sustainable approach to contact tracing and resulting social isolation. Continuing financial support will need to be available to ensure that the population is able to comply with digital contact tracing instructions.

3. Criminality and scams

People might create fake versions of official digital contact tracing services for profit. Google and Apple have been vetting coronavirus services before they can be added to the app store but people may be tricked into clicking links spread through other routes. Government will need to be vigilant and work closely with internet crime specialists to stop potentially harmful behaviour.

35 Good Things Foundation. (2019). Digital Nation 2018. *Goodthingsfoundation.org*. Available from: https://www.goodthingsfoundation.org/research-publications/digital-nation-2018 [Accessed 16.4.20].

Recommendations

Finding: There is currently insufficient evidence to support the use of digital contact tracing as an effective technology to support the pandemic response. The technical limitations, barriers to effective deployment and social impacts demand more consideration before digital contact tracing is deployed.

Recommendation: Government must establish an independent Group of Advisors on Technology in Emergencies to oversee the development and testing of any prospective digital contact tracing app. The Group of Advisors should be charged with adjudicating when a digital contact tracing app is ready for deployment, taking into consideration:

- Evidence establishing the need for digital contact tracing to support manual contact tracing;
- The widespread availability of coronavirus testing for the general population;
- The potential for the app to achieve wide and consistent use among more than 60% of the population;
- A comprehensive understanding of the data architecture underpinning the app.

The remit of the Group of Advisors must include the ability to stipulate:

- The parameters against which the risk-scoring algorithm integrated into the digital contact tracing app detects and scores contacts;
- What technical features a digital contact tracing app should have in order to render the most useful data;
- What design features a digital contact tracing app should have in order to make it accessible and ensure compliance with its instructions;
- Privacy-preserving measures that the digital contact tracing app should integrate.

Finding: If a digital contact tracing app is approved for deployment, it will only be effective if used as a tool to supplement and assist manual contact tracing (performed by medical professionals on the basis of interviews with patients) and if based on confirmed diagnostic tests for the virus.

Recommendation: Resources must not be diverted from manual contact tracing or diagnostic testing to technology development. The deployment of a digital contact tracing app should be delayed until system capacity for testing and manual contact tracing is increased sufficiently to meet an increase in demand caused by the roll-out of the app. Testing and manual contact tracing capacity must be sufficient to cover those segments of the population who are digitally excluded because of their age, disability, vulnerability, device ownership or digital literacy.

Finding: The effectiveness of a digital contact tracing app will be contingent on widespread public trust and confidence, which must translate into broad adoption of the app.

Recommendation: In order to increase public trust and confidence, and guard against abuse and scope creep, Government should advance primary legislation to:

- Set out the limited purposes for data processing;
- Limit who has access to data and for what purpose;
- Require the deletion of data after specified periods, as well as exemptions from deletion of anonymised data for the use in research;
- Require the performance, publication and approval by the Information Commissioner's Office of a data protection impact assessment for all technical measures to support the crisis;
- Establish a power for the Information Commissioner's Office to develop a Code of Practice pertaining to the processing of data within the context of the crisis.

Legislation should also contain safeguards making uses of data in contravention of regulation unlawful. Such uses would include:

- Use as evidence in the adjudication or imposition of civil or criminal sanctions;
- Use in proceedings or adjudications relating to visa or immigration status or rights;
- Use in family or child proceedings;
- Use in any other types of legal proceedings;
- Use to support any actions for denial of welfare or other public or social benefits;
- The sharing of data with employers or insurers without the freely given consent of the individual;
- The reliance on data by an employer to terminate or alter the existing conditions of employment or service;
- The use to discriminate in a way that would be illegal under the Equality Act 2010.

Finding: Given the lack of evidence as to the effectiveness of digital contact tracing, there is no basis to conclude that a mandatory requirement to install a digital contact tracing app would be necessary or proportionate. From a pragmatic standpoint, mandating use of a digital contact tracing app is unlikely to be effective, enforceable or enjoy public support.

Recommendation: If the Group of Advisors recommends the deployment of a digital contact tracing app, it should consider what steps the Government could take to increase voluntary public adoption of the app, through incentives or automatic app updates pushed to users' devices.

4. Symptom tracking

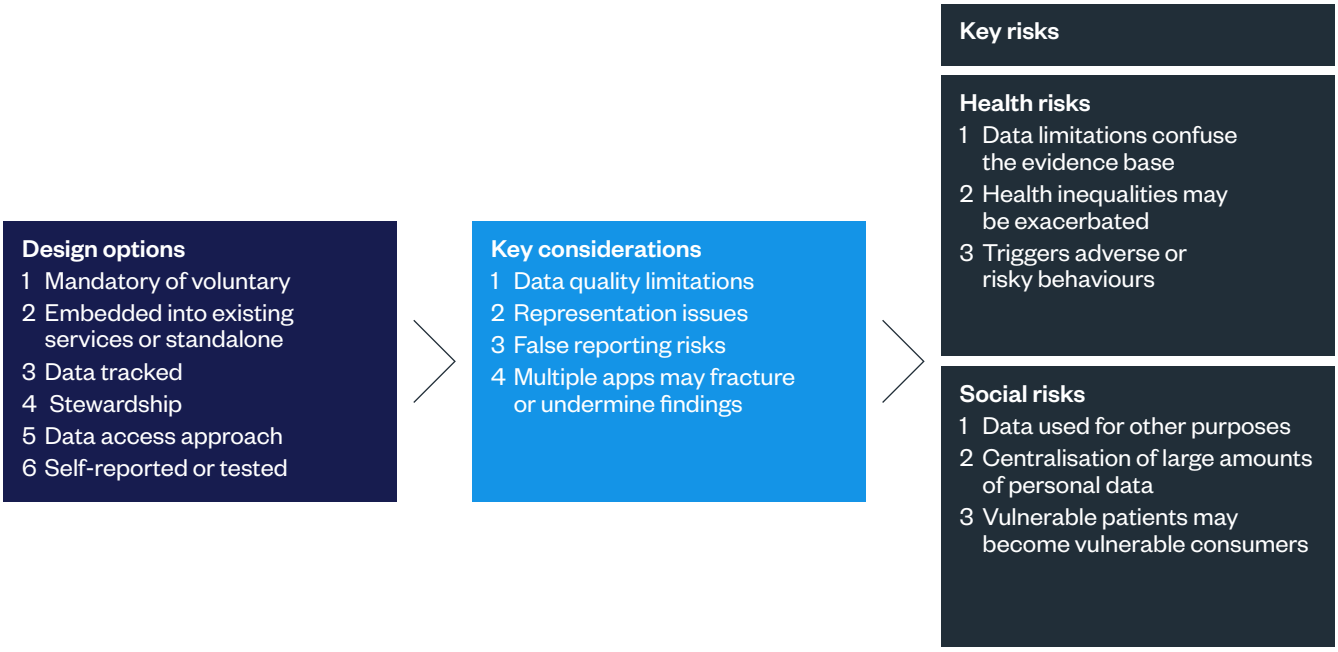

Chart 4
Overview of digital symptom tracking

Public health authorities and medical researchers need to understand how and where people are experiencing the coronavirus disease. This helps them to plan healthcare responses such as where and when medical capacity may be required, how to detect the virus, or to understand the lifecycle of the virus in patients and what risk factors exist. It can help politicians and public health authorities to understand what effect social measures such as lockdown and social distancing are having in reducing the spread of the virus.

Information about symptoms has primarily come from clinical settings, but the public are increasingly being asked to report symptoms themselves through various apps to support timeline information gathering without burdening the health system.

How does it work?

Symptom tracking services take the form of apps and websites that encourage citizens to share some information about themselves (such as their age, gender and medical history), and report their symptoms, usually on a regular basis such as once a day. The data is collected by an organisation that makes it available for research by one or many organisations. That research then contributes to responses to the pandemic.

Design options

Technical measures are already being deployed to help patients report symptoms. A number of approaches are emerging, with different features. Breaking down the characteristics of symptom tracking applications assists in identifying potential issues areas:

1. Mandatory or voluntary

Some governments have made symptom tracking mandatory under some circumstances. People who are quarantined in South Korea have to report their symptoms twice a day. They can choose whether to do this through a government supplied app or by telephone contact with a local government official.[36]

2. Form of service: embedded into existing services, or in a new standalone app

Symptom tracking might be embedded into existing services as a 'side-effect' of an existing service, for example digital thermometers and other personal health devices[37] or new apps might be developed explicitly for this purpose. In England[38] the NHS have prominently placed a symptom tracking service on their COVID-19 information pages, while researchers at Carnegie Mellon University have worked with Facebook and Google to place a survey into people's Facebook newsfeed and Google's Opinion Rewards app.[39, 40, 41] Alternatively symptom tracking might be a new standalone service, such as the collaboration between King's College London, Guys and St Thomas' Hospitals working in partnership with ZOE Global Ltd – a health science company – on the COVID-19 symptom tracker.[42] This is a standalone app that users download and enter symptom information into.

36 Kim, M. (2020). South Korea is watching quarantined citizens with a smartphone app. *MIT Technology Review* [Online]. Available from: https://www.technologyreview.com/2020/03/06/905459/coronavirus-south-korea-smartphone-app-quarantine/ [Accessed 16.4.20].

37 Bazzoli, F. (2020). Digital thermometer data may provide insight into COVID-19 surges. *Healthcare IT News* [Online]. Available from: https://www.healthcareitnews.com/news/digital-thermometer-data-may-provide-insight-covid-19-surges [Accessed 16.4.20].

38 At the time of writing the symptom tracking service was not visible on the websites of NHS in devolved UK nations.

39 See the Nhs.uk *Coronavirus Status Checker* webpage at: https://www.nhs.uk/coronavirus-status-checker [Accessed 16.4.20].

40 Jin, K.X., McGorman, L. (2020). Data for good: new tools to help health researchers track and combat COVID-19. *Facebook*. Available from: https://about.fb.com/news/2020/04/data-for-good/ [Accessed 16.4.20].

41 Dave, P. (2020). Google asks users about symptoms for Carnegie Mellon coronavirus forecasting effort. *Reuters* [Online]. Available from: https://www.reuters.com/article/us-health-coronavirus-google/google-asks-users-about-symptoms-for-carnegie-mellon-coronavirus-forecasting-effort-idUSKBN21B09Q [Accessed 16.4.20].

42 See the *COVID Symptom Tracker* 'about' page at: https://covid.joinzoe.com/about [Accessed 16.4.20].

3. Data tracked

All symptom trackers will collect demographic data about the participant (for example age, gender), information about their past medical history, as well as approximate geographic location, and a time series of data about their symptoms. The data about their symptoms might include information about tests that have been performed, whether they have a cough, or whether they have a high temperature. Some organisations have started to develop a standard for this data.[43] Some trackers may collect more information about an individual, for example a survey on Facebook could collect a Facebook profile name, while a web survey might capture IP and email address.

4. Stewardship

Each symptom tracker will have an organisation that is the data steward, which makes decisions about who can access what type of data, for what purposes and under what conditions. For the NHS Symptom Tracker this is NHS England, a regulated body with established data governance processes, relationships with a range of researchers and known accountability measures. For the COVID-19 Symptom Tracker this is King's College London, although the app's privacy policy notes that the data will be shared with a range of research institutions both in the UK and abroad.

5. Data access approach

In conjunction with NHS Digital an aggregated version of the NHS Symptom Tracker data, such as the number of people tracking symptoms in geographic areas, is being made openly available to inform decision making, while more detailed data is being securely shared to appropriately authorised researchers.[44] This is individual level data which is potentially re-identifiable. The team behind the COVID-19 Symptom Tracker app is publishing blog posts with analysis of the data it is collecting but do not appear to be sharing the detailed data with the NHS at this stage.[45]

6. Context of use: self-reported or tested

Most symptom tracking apps currently in use in the UK are using self-reported symptoms. In other contexts, such as South Korea, there are mandatory apps for individuals with confirmed cases of COVID-19 operating alongside voluntary self-reporting apps.

---

43 See *[Draft] International open data standard for COVID-19: community case reporting / surveys; symptom trackers; testing services* at https://docs.google.com/document/d/1XjKrimQHjnATctZliuqdaqfc0daiq6tlcFddSupPg60 [Accessed 16.4.20].

44 See the data set on the NHS Digital website at: https://digital.nhs.uk/coronavirus/nhs-111-online-coronavirus-services/potential-coronavirus-symptoms-reported-through-nhs-pathways-and-111-online [Accessed 16.4.20].

45 For example, see 'The impact of self-isolation' on the *COVID Symptom Tracker* website Covid.joinzoe.com. Available from: https://covid.joinzoe.com/post/covid-isolation [Accessed 16.4.20].

Symptom tracking service	Mandatory or voluntary	Form of service	Types of data	Data steward	Data access	Context of use
NHS Symptom Tracker	Voluntary	Website	Symptoms plus basic demographic data	NHS England	Aggregated open data, detailed data shared with researchers	Self-reported when individuals visit NHS website
COVID-19 Symptom Tracker	Voluntary	App	Symptoms, basic demographic data and email address	King's College London	Aggregate data and analysis shared in articles	Self-reported through smartphone
South Korean government 's symptom tracking app (Multiple voluntary self-reporting apps also exist)	Mandatory	App or phone	Symptoms tied to individual	Public health authority	Unknown	Self-reported twice daily entry while in quarantine following positive test or following arrival in country
Taiwan government's symptom tracking app (Multiple voluntary self-reporting apps also exist)	Mandatory	App or phone	Symptoms tied to individual	Public health authority	Unknown	Self-reported twice daily entry while in quarantine following positive test or following arrival in country

Table 2
Comparison of proposed international digital symptom tracking apps

Decisions taken about the approach for symptom tracking will affect the quality of the information being collected.

Key considerations

1. Data quality

Symptom tracking data will vary in quality based on who is collecting it, where they are collecting it and the context within which it is being collected. Given the very limited testing, the likelihood is much of the data will rely on self-reporting, which is particularly problematic for COVID-19 given its novelty, a high proportion of asymptomatic cases, and the large variety of symptoms many of which are the same as other common illnesses. This may limit the reliability of the data and its value to researchers and public health professionals for some aims (although not all).

2. Representation

Second, the symptom data will not be representative of the population and hence create imbalances in data in terms of demographics, geography and socio-economic vulnerability. This can lead to an inequitable distribution of benefits from government activity and a deprived research base for certain populations.

3. False reporting risks

There will be incentives for false reporting if there is a consequence for the member of the public due to the symptom data, for example someone who is in a self-enforced quarantine may claim that they are healthy so that they can be released to see their family. This can affect the utility of the data and points to the need for wide consideration of the interaction between different public health measures.

4. Multiple apps may fracture or undermine findings

Symptom data from one app may contain different fields from a different app. The user experience and content on each app can affect how a citizen enters their symptoms.

Analytical methods can help researchers counteract these different effects. Tracking the provenance of each source of symptom data, the designs of each app, and the context in which it is used will help produce higher quality research.

Risks and impacts

The risks and impacts of symptom tracking apps fall into two broad categories: health risks and data protection risks.

Health risks

- **Data limitations confuse the evidence base**: Multiple competing symptom trackers that do not safely share data will inhibit the ability of public health professionals to obtain a complete picture of the symptom tracking population, let alone the entire population. Symptom tracking will not spot people who are asymptomatic, and datasets may be skewed by inaccurate reporting or deliberate attempts to poison the well of data with false data. Different organisations might not follow medical guidelines and may collect symptom data that is not useful for the intended purpose.

- **Health inequalities may be exacerbated**: Most people who are comfortable with digital services are younger, more tech savvy, and comparatively affluent and the language, design and promotional activity around apps may attract certain demographic groups. This risks building a skewed data picture, especially as those at risk, directly and indirectly, are the elderly and those with underlying health conditions, who may be less likely to participate. There is a real risk of exacerbating inequalities of understanding and responding effectively for certain groups. For example, initial data published by the COVID-19 Symptom Tracker app demonstrates a concentration of the 1,325,000 users of the app (as at end of March 2020) in the south of England, and a paucity of users in Northern Ireland.[46]

- **Symptom tracking may trigger risky or adverse behaviours**: The process of capturing symptoms might lead someone to conclude that they falsely have the virus, or that they do not have the virus when they do. This may lead to individuals displaying risky or overly cautious behaviour because of inaccurate 'diagnoses'. Entering symptom data may give people a false sense of security about their health and undermine other measures, such as enforced social distancing measures.

Social risks arising from data collection

- **Data may be shared more widely and platforms may be repurposed**: An individual might be affected by future use of the data, for example in a recruitment or insurance service where the symptom data might unfairly reveal information about an individual that they have the right not to share with those organisations. An employer may try to demand an individual discloses information from their symptom tracking app as a requirement to return to work.

- **Symptom tracking databases centralise large amounts of personal data**: By acquiring and collating personal data, including sensitive health data, symptom tracking databases may become 'honeypots' prone to adversarial attacks and breaches. In particular, where symptom tracking apps collect more data than is needed for the service, this may make data subjects more vulnerable to data breaches, malicious attacks on large datastores, or otherwise undermine trust and confidence in the service, deterring people from reporting symptoms.

- **Vulnerable patients may become vulnerable consumers**: The organisation collecting the symptom data might prove to be untrustworthy by monetising the data and the inferences it draws about participants. It might keep the data and use it after the crisis is over for advertising or other purposes.

46 Anonymous. (2020). Who are the 1.5 million citizen scientists?. *Covid.joinzoe.com*. Available from: https://covid.joinzoe.com/post/uk-covid19-trackers [Accessed 16.4.20].

Some of these risks may fall foul of data protection legislation, employment and equalities law. In particular, collection of non-essential data and its use for purposes other than those strictly defined by the app would contravene the data protection principles of purpose limitation and data minimisation.

Other risks can be mitigated, but potential mitigation measures themselves have impacts that need to be considered. Below, we have colour-coded mitigation measures red or green according to their feasibility.

Health risk	Mitigation measures	Impact
Data limitations confuse the evidence base	Make a single symptom tracking service compulsory to download and use	Requiring compulsory use of a symptom tracking app is unlikely to be regarded as a proportionate interference with individual rights, particularly given the concerns about the quality of the data collected through self-reporting
	Only permit use of symptom tracking apps for individuals who receive a positive test for the virus	Until a widespread programme of testing is available for the general public, this would dramatically diminish the numbers of users and therefore the evidence available to researchers
	Create and promote an open standard to enable interoperability across services	Scientific research into COVID-19 symptoms is ongoing and new symptoms are being identified The standard will need to have the capability to be updated, while tolerating a level of divergence to help with the discovery of new symptoms
	Require oversight by the Medicines and Healthcare products Regulatory Agency (MHRA). MHRA could publish a set of guidelines for symptom tracking services, provide an approvals process, and provide a statement on how they are being audited to reduce the chance of misuse	Unless expedited, this could unnecessarily slow down the collection of symptom tracking data leading to delayed public health benefits
Health inequalities may be exacerbated	Analyse data to understand representation and create targeted strategies to collect data from underrepresented groups	Although this will have time and cost implications, given the likelihood that the pandemic will be sustained for some time, this is a critical mitigation measure
	Require PHE to publish information on the representativeness of datasets	Although this will have time and cost implications, given the likelihood that the pandemic will be sustained for some time, this is a critical mitigation measure
Symptom tracking may adversely affect individual behaviour	Provide design guidelines for symptom tracking services based on user research into behavioural effects	Although this will have time and cost implications, given the likelihood that the pandemic will be sustained for some time, this could be a useful mitigation measure
	Promote continued compliance with social distancing measures as part of general communications strategy	This is consistent with the crisis response in any event

Table 3
Feasibility and impact of mitigation measures to offset health risks of symptom tracking apps

Data risk	Mitigation measures	Impact
Data handed over for one purpose may be used for others	Government could issue guidance emphasising strong purpose limitation measures on data collected by symptom tracking apps	Needs to be complemented with auditing and enforcement to have desired effect
More data may be collected than is needed for the service	Government could issue guidance discouraging developers from collecting data which isn't strictly necessary for the functioning of the app	Needs to be complemented with auditing and enforcement to have desired effect
Vulnerable patients may become vulnerable consumers	Government could require the deletion of data after a minimum period of time (reviewable on application to the Information Commissioner's Office)	Ongoing public health and medical research may require access to the data This could be achieved through anonymisation and the imposition of obligations not to deliberately reidentify individuals

Table 4
Feasibility and impact of mitigation measures to offset data risks of symptom tracking apps

Recommendations

Finding: Of the three technologies considered in this rapid evidence review, symptom tracking raises the fewest risks and concerns, but also has the most limitations in terms of data quality, coverage and accuracy.

Recommendation: Government should support and foster public trust in symptom tracking efforts by strengthening the governance landscape in which they are being deployed. Government should advance primary legislation to:

- Set out the limited purposes for data processing;
- Limit who has access to data and for what purpose;
- Require the deletion of data after specified periods, as well as exemptions from deletion of anonymised data for the use in research;
- Require the performance, publication and approval by the Information Commissioner's Office of a data protection impact assessment for all technical measures to support the crisis;
- Establish a power for the Information Commissioner's Office to develop a Code of Practice pertaining to the processing of data within the context of the crisis.

Legislation should also contain safeguards making uses of data in contravention of regulation unlawful. Such uses would include:

- Use as evidence in the adjudication or imposition of civil or criminal sanctions;
- Use in proceedings or adjudications relating to visa or immigration status or rights;
- Use in family or child proceedings;
- Use in any other types of legal proceedings;
- Use to support any actions for denial of welfare or other public or social benefits;
- The sharing of data with employers or insurers without the freely given consent of the individual;
- The reliance on data by an employer to terminate or alter the existing conditions of employment or service;
- The use to discriminate in a way that would be illegal under the Equality Act 2010.

5. Immunity certification

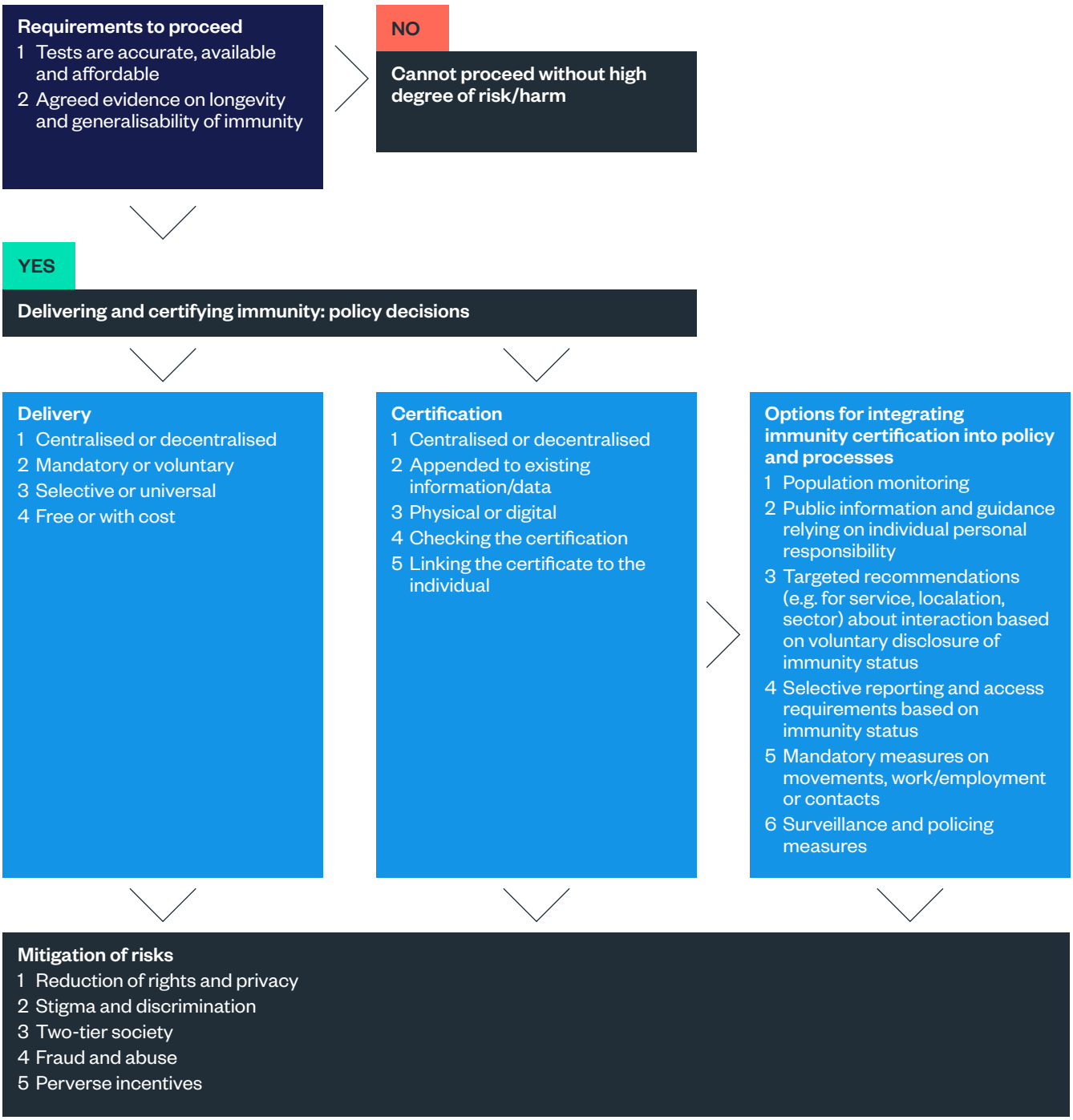

Chart 5
Overview of digital immunity certification

There is broad agreement that widespread testing is the only route through which the UK can exit the coronavirus crisis, and the UK has highlighted immunity testing as a key strategy.[47] Testing will enable the identification of the virus and the spread of immunity throughout the population. People, businesses, public health authorities and governments want to know who is immune to the virus so that they can return to work, care for other vulnerable people, and participate in the post-crisis reconstruction. Immunity is particularly important for people in high risk services such as health and social care.

There is not yet evidence to confirm that long- or short-term immunity to COVID-19 can be established either through contracting the virus or through a vaccine. Assuming such evidence emerges, and credible immunity tests could be established, or a vaccine is created, then a means for certifying immunity may need to be developed. Immunity certificates may not need to form part of an immunity testing strategy, but Health Minister Matt Hancock has referenced the government's interest in developing immunity certificates, and other countries are investigating the potential for immunity passports. The United States government is reportedly in talks with a British AI company Onfido to develop biometric digital immunity certification technology.[48] There is anecdotal evidence to demonstrate some private providers in the UK are already offering immunity certificates.

Digital technologies may provide the most secure means of certifying an attribute such as immunity, because of the protections they provide from fraud, theft, and abuse. However, digital immunity certification is a highly complex and controversial policy intervention; by analogy, the digital-only settled status scheme provoked calls from advocacy groups for the UK government to provide physical documents to evidence immigration status.[49]

There are no clear proposals for immunity certification technologies 'on the table'. This section of this review differs from the preceding two in that respect. Nevertheless, we think it possible that existing or proposed symptom tracking and digital contact tracing applications will be expanded or repurposed to support an immunity certification regime. This would be a problematic expansion of scope and it warrants surfacing some of the considerations and concerns raised by such a regime here.

Before discussing the technical measures for implementing immunity certification, it is essential that the limitations of immunity testing are acknowledged, and a range of sequential questions are asked and options interrogated. We have structured this section to provide a roadmap for policymakers thinking about implementing an immunity certification regime.

---

47 Professor Sir John Bell outlines the issues around testing in Bell, J. (2020) Trouble in testing land. *Research.ox.uk*. Available from: https://www.research.ox.ac.uk/Article/2020-04-05-trouble-in-testing-land See also, Blair, T. (2020). The UK has no route out of Coronavirus crisis without mass testing. *The New Statesman* [Online]. Available from https://www.newstatesman.com/politics/uk/2020/04/uk-has-no-route-out-coronavirus-crisis-without-mass-testing Costello, A. (2020). Mass testing is the only way to stop the virus – it's long overdue. *The Guardian* [Online]. Available from: https://www.theguardian.com/commentisfree/2020/mar/25/mass-covid-19-testing-is-vital-but-the-data-must-be-localised Pancevski, B. (2020). Some nations look to mass testing for faster way out of Coronavirus. *Wall Street Journal* [Online]. Available from: https://www.wsj.com/articles/some-nations-look-to-mass-testing-for-faster-way-out-of-coronavirus-crisis-11585758518 [All accessed 16.04.2020].

48 Coulter, M. (2020). The US government is to roll out immunity passports for those recovered from COVID-19. *Business Insider* [Online]. Available from: https://www.businessinsider.com/coronavirus-onfido-immunity-passports-2020-4?r=US&IR=T [Accessed 16.4.20].

49 O'Carroll, L. (2020). Unsettled status: EU citizens want card to prove right to stay in UK. *The Guardian* [Online]. Available from: https://www.theguardian.com/uk-news/2020/jan/20/unsettled-status-eu-citizens-want-card-to-prove-right-to-stay-in-uk [Accessed 16.4.20].

Step one: Is the science on immunity sufficiently robust so as to warrant a policy approach centred on immunity certification?

An effective policy focused on immunity certification will require:

1. A sufficiently accurate and reliable test for current immunity, which meets the requisite standards in terms of sensitivity (the proportion of people with the disease who will get a positive test) and specificity (the proportion of healthy people without the disease who will get a (correct) negative test);[50]
2. Evidence as to the longevity and generalisability of immunity; and
3. An available and affordable test for immunity that can be mass produced and widely disseminated.

Currently no country has widespread use of immunity tests which meet acceptable levels for sensitivity and specificity.[51] The novelty of the virus means there is not yet consensus on the length of immunity – it will be nine more months before we know if it can last a year – and critically whether immunity varies for different groups of people.

The science will improve against all of these three conditions, however it is critical that policy doesn't overreach given the risks of incorrect assumptions of immunity. Even the best performing tests will still return a number of false positives, so it is vital that public authorities help people understand and communicate the statistics that indicate how useful an immunity test is.[52] While 95% or 90% accuracy rate might be acceptable for many people and for other illnesses, it might be considered too great a risk for those interacting with shielded patients, for example, given the disease's high levels of transferability and poor prognosis. It may be useful to establish different levels of confidence in immunity that are useful for different purposes.[53]

50 Understanding the true meaning of a positive or negative test will also require knowledge of the prevalence of the infection in a given community. This is as yet unknown (and one of the aims of such testing) and therefore these elements of testing will not be known for some time, making any assessment of the true likelihood of disease in the event of a positive test (or likelihood of no disease in a negative test) limited.

51 Patel, N. V. (2020). Why it's too early to start giving out "immunity passports". *MIT Technology Review*. Available from: https://www.technologyreview.com/2020/04/09/998974/immunity-passports-cornavirus-antibody-test-outside/ [Accessed 16.4.20].

52 These are similar issues to those explored by David Spiegelhalter and Kevin Mcconway in relation to facial recognition systems: Spiedelhalter, D. Mcconway, K. (2020). Live facial recognition: how good is it really? We need clarity about the statistics. *Winton Centre for Risk and Evidence Communication, University of Cambridge*, on *Medium.com*. Available from: https://medium.com/wintoncentre/live-facial-recognition-how-good-is-it-really-we-need-clarity-about-the-statistics-5140bd3c427d [Accessed 16.4.20].

53 Kriendler, J. (2020). Must we wait for the perfect COVID immunity test? *Medium.com*. Available from: https://medium.com/@phantom.medic/must-we-wait-for-the-perfect-covid-immunity-test-f2eb4b910dc [Accessed 16.4.20].

Excerpt from 'Advice on the use of point-of-care immunodiagnostic tests for COVID-19: Scientific Brief', published by the World Health Organisation on 8 April 2020

There is [a] [...] rapid diagnostic test marketed for COVID-19; a test that detects the presence of antibodies in the blood of people believed to have been infected with COVID-19. Antibodies are produced over days to weeks after infection with the virus. The strength of antibody response depends on several factors, including age, nutritional status, severity of disease, and certain medications or infections like HIV that suppress the immune system. In some people with COVID-19, disease confirmed by molecular testing (e.g. reverse transcription polymerase chain reaction: RT-PCR), weak, late or absent antibody responses have been reported. Studies suggest that the majority of patients develop antibody response only in the second week after onset of symptoms. This means that a diagnosis of COVID-19 infection based on antibody response will often only be possible in the recovery phase, when many of the opportunities for clinical intervention or interruption of disease transmission have already passed.

Antibody detection tests targeting COVID-19 may also cross-react with other pathogens, including other human coronaviruses, and give false-positive results. Lastly, there has been discussion about whether RDTs detecting antibodies could predict whether an individual was immune to reinfection with the COVID-19 virus. There is no evidence to date to support this.

Tests to detect antibody responses to COVID-19 in the population will be critical to support the development of vaccines, and to add to our understanding of the extent of infection among people who are not identified through active case finding and surveillance efforts, the attack rate in the population, and the infection fatality rate. For clinical diagnosis, however, such tests have limited utility because they cannot quickly diagnose acute infection to inform actions needed to determine the course of treatment.

Some clinicians have used these tests for antibody responses to make a presumptive diagnosis of recent COVID-19 disease in cases where molecular testing was negative but where there was a strong epidemiological link to COVID-19 infection and paired blood samples (acute and convalescent) showing rising antibody levels.

Based on current data, **WHO does not recommend the use of antibody-detecting rapid diagnostic tests for patient care but encourages the continuation of work to establish their usefulness in disease surveillance and epidemiological research**.

References have been removed from the above text for brevity. They can be found in the original version: https://www.who.int/news-room/commentaries/detail/advice-on-the-use-of-point-of-care-immunodiagnostic-tests-for-covid-19

Step two: How would immunity testing be delivered?

Assuming immunity could be robustly established through testing, the Government will need to develop a comprehensive strategy on immunity testing and certification.

Once a test has been approved then it will need to be distributed. This will involve decisions about who is prioritised to be tested, how much it will cost, how a test will be distributed, and how many times (or how frequently) an individual should or can be tested.

In California testing is provided by Verily, a Google subsidiary, and requires citizens to create a Google account.[54] Even a relatively small barrier like this might exclude some people from getting the test.

In the UK it has been briefed that some of the logistics may be provided by private sector logistics firms such as Royal Mail, Amazon and Boots.[55] A mixed model is likely to emerge where the private sector provides accredited tests for a fee and the public sector provides tests for free, but prioritises who has access to them and uses private sector logistics firms to deliver them.

The strategy will need to specify whether immunity testing will be:

1. Centralised or decentralised

Given the already-strained capacity of the National Health Service, it is unlikely it could take on a new national function of immunity testing at the scale necessary to cover the entire population within a reasonable time period. As such, it is likely that testing will need to be decentralised and conducted through private providers, or mass-produced for at-home testing. Government policy will need to ensure a standardised approach to immunity testing across private providers, either through mandating a specific test or a specific approach, in order to avoid deterioration in the robustness of the approach and a resulting lack of trust in immunity testing.

2. Mandatory or voluntary

Government-mandated immunity testing would constitute a severe infringement on personal liberty and privacy. It would need to be accompanied by the most stringent of regulatory protections, and would have to be provided free-of-charge. However, it is unlikely to be necessary; if it were free and enabled peace of mind and unimpeded access to movement and services, it is likely it would be taken up by the majority of the population.

54 Greenwood, F. (2020). Google wants your data in exchange for a coronavirus test. *Foreign Policy* [Online]. Available from: https://foreignpolicy.com/2020/03/30/google-personal-health-data-coronavirus-test-privacy-surveillance-silicon-valley [Accessed 16.4.20].

55 ITV News. (2020). Firms including Amazon and Boots to help UK reach target of 100,000 coronavirus tests per day. *ITV News* [Online]. Available from: https://www.itv.com/news/2020-04-02/amazon-to-help-uk-reach-new-target-of-100-000-coronavirus-tests-per-day-by-end-of-april [Accessed 16.4.20].

3. Selective or universal

Depending on the testing capacity developed, access to immunity testing is likely to be prioritised for certain groups, chiefly key workers to preserve their own safety and the integrity of those services. Beyond key workers, and in step with the Government's exit strategy, individuals working in certain sectors could be prioritised over others – prioritisation might be given to important sectors to get society and the economy running again. Those personally interacting with shielded patients or vulnerable persons might also be prioritised to enable them to access services they require.

4. Free or with cost

Tests could be free, free for some (key workers), matched to NHS prescription costs (free for low income or high risk groups) or provided with a charge. Any cost would affect coverage.

Step three: How would immunity testing be certified?

Testing alone will be ineffective without a means by which tested individuals can certify their immunity. Immunity certification can be recorded in one or more places. These can be loosely grouped into centralised and decentralised locations.

- Centralised locations
  - Digitally recorded in an NHS personal health record[56]
  - Digitally recorded in other health information systems (like the Child Health Information System)
  - Digitally recorded in other government information systems (for example passport or welfare systems)
  - Digitally recorded in a new central database (for example the new NHS Coronavirus data store)

- Decentralised locations
  - Physically recorded on new physical documentation (like yellow fever)
  - Physically appended to existing state-provided physical documentation (for example passports)
  - A digital token on a smartphone
  - A digital attribute as part of a (new) digital identity system

56 NHS. (2018). Your health records. *Nhs.uk*. Available from: https://www.nhs.uk/using-the-nhs/about-the-nhs/your-health-records/ [Accessed 16.4.20].

How would digital immunity certification work?

Details of the immunity status of an individual will need to be shared with a third party (the 'relying party') who will take actions on the basis of the claims made in that person's immunity certificate. For example, this 'relying party' may decide that the individual may only be allowed to enter a restaurant if they can establish their immunity. Similarly, checking an individual's immunity might be an important stage in the process of employment in future.

A digital immunity certificate might be stored locally, under the control of the individual on their personal device, or centrally (on a centralised database).

Checking the certificate

The process of checking the individual's immunity certification could take a variety of forms, depending on where the certifications were stored, who has control over access to the certification and what kind of audit trails about the checking are deemed necessary and appropriate.

In the case of physical documentation under the direct control of the individual, the checking would be undertaken by physically inspecting the documentation. This approach is dependent on the relying party being aware of, and able to check for, fraudulently produced documents.

Storing the certificate digitally on a personally controlled device provides stronger assurance that the certificate has not been compromised or fraudulently produced and its checking can be automated. In such scenarios, it is not necessary to create a central audit trail of when (and where) the immunity certification was checked.

If the digital certification is held centrally, for example in an NHS record, this would involve relying parties being able to access the electronic record for the particular individual. This might be implemented via an Application Programming Interface (API) that provides a simple yes / no answer to the question of whether a certificate exists for the specific individual (i.e. they are currently immune), in a similar way to which the GOV.UK Document Checking Service allows companies to check whether passport details are valid and have not been reported lost or stolen.[57]

A more sophisticated API might also return more detailed information such as when the person was tested, who they were tested by and what the test results showed. This API might be particularly appropriate for primary care scenarios.

Linking the certificate to the individual

A key consideration for either approach, however, is linking the immunity certification to the person who was tested. Being certified as being immune could open up significant advantages to individuals, for example, by allowing them to take up particular work opportunities, travel, etc. This means there is a real risk of fraud where individuals try to get access to immunity certification that does not apply to them.

Assuming that the testing process itself is robust, fraudulent activities might take the form of creating faked physical documentation (which is much more difficult to achieve with digital documentation) or linking correct test results to a different person. A key step, therefore, is securely binding the test results to the person who was tested; linking the attribute to the identity.

57 Whitley, E. A. (2018). Trusted digital identity provision: GOV.UK Verify's federated approach. *Centre for Global Development*. Available from: https://www.cgdev.org/publication/trusted-digital-identity-provision-gov-uk-verify-federated-approach [Accessed 16.4.20].

In the case of physical documentation, this might involve including personal details (face image or name and address) on the certification and then also checking this against the person presenting the documentation. Alternatively, it may be possible to link the ownership of the device to the test results (perhaps by also including a fingerprint or face biometric). However, this can cause problems for lost or stolen devices or a change of device after the test was taken.

Another option is to link the immunity certification attribute to an independently verified identity. For a centralised store of the certificates, this would require confirming the identity of the individual before checking the attribute via the API. For certificates held on a personal device, the individual might need to satisfy appropriate authentication requirements,[58] for example, by using their face or fingerprint to unlock the device.

Step four: How would immunity certification be integrated into policy and processes?

If the preceding steps could be safely achieved, policy interventions could be built around immunity certification. These could span from voluntary, non-intrusive measures to mandatory and highly intrusive measures, and could include one or more of:

- The aggregate monitoring of the spread of immunity across the population to support health approaches.
- Public information and guidance at an individual level to accompany immunity testing, relying on individual personal responsibility to shape behaviour.
- Recommendations developed at service, area or sector level, for example to offer flexibility or additional protections for those without immune status in high risk areas or in contact with vulnerable groups (for example taking individuals away from front line duties where possible).
- Selective reporting requirements (to access certain areas or to undertake types of employment).
- Mandatory restrictions on movement, work/employment or contact with others for non-immune groups and/or requirements for immune groups to undertake certain types of service.
- Surveillance measures based on immunity (tracking movement or compliance with other measures).

58 UK Cabinet Office. (2014). Authentication credentials for online government services. *Gov.uk*. Available from: https://www.gov.uk/government/publications/authentication-credentials-for-online-government-services [Accessed 16.4.20].

Even if a centralised immunity certification regime is deployed, independent initiatives may proliferate (and indeed already are). Private sector actors may choose to develop their own immunity certification systems, and actors across the economy may choose to recognise non-government certification. In China, for example, the Alipay Health Code app enables individuals to obtain a score as to their health status, and cafes, restaurants and public transport systems recognise that health status as a form of certification.

Independent initiatives will need to be restricted or regulated in order to prevent public trust in certification being undermined by false or untrustworthy initiatives. Standardisation will become increasingly important, and these standards will need to be openly developed so that they can learn from emerging best practices.

Mitigation of risks

1. Restriction of individual rights, particularly privacy

An immunity certification regime established by the Government for one end – for example, to enable monitoring of immunity to support public health interventions – could be adopted and used for a range of other ends. Employers could require employees demonstrate immunity to return to work, food delivery services could require customers to establish immunity before placing orders, or cafés could ask for immunity certification on entry.

Government will need to contemplate these potential secondary uses of an immunity certification regime and ensure they are proportionate and provided for in regulation. Will it be legal to check immunity before someone gets a job where they can work from home? Before someone enters a hospital? Legislation, such as the Equalities Act, provides a range of protections against discrimination but Government may need to actively allow some discrimination against individuals under a clearly defined set of circumstances to create the desired public health outcome of saving lives.[59]

59 UK Government. (2010). Equality Act 2010. *Legislation.gov.uk*. Available from: http://www.legislation.gov.uk/ukpga/2010/15/contents [Accessed 16.4.20].

2. Stigmatisation and discrimination

Checks will not just occur in establishments. People can be expected to try to check each other's immunity. This can lead to other forms of discrimination. As Pete Mills observes 'it cannot be ignored that, throughout the UK's COVID-19 epidemic, there have been sporadic reports of low-level discrimination and hate crime'.[60] This is a pandemic, so discriminatory behaviour can be driven by fear as well as hate.

Government will also need to consider the longer-term discriminatory implications of immunity verification. Will it form part of future checks in employment and insurance services? Or even online dating services? What will happen if a reliable immunity test is never developed? Or if an acceptable immunity test is developed, but no reliable vaccine for COVID-19 is developed?

3. A two-tiered society

Decisions about how certification is prioritised may undermine current sense of solidarity and equity. If groups face barriers (because or rural location, or cost for example) this could exacerbate disadvantage

An immunity certification regime risks creating a two-tiered system as we exit the pandemic, whereby the immune are able to return to work, move freely and enjoy unrestricted activities while the ill, not-yet-immune, or not-immune are placed under onerous restrictions.[61] This may result in stigmatisation of those without immunity, who may also suffer from social and financial disadvantage by being denied work and movement. Guidance to employers, public benefits and support, and alterations to the health service will all be necessary to ensure a sustainable approach to an immunity certification regime.

60 Nuffield Council on Bioethics. (2020). Liberty, solidarity and the biopolitics of COVID-19. *Nuffieldbioethics.org*. Available from: https://www.nuffieldbioethics.org/blog/liberty-solidarity-and-the-biopolitics-of-covid-19
Guttridge, R. (2020). Two coronavirus hate crimes a week reported to police. *Express & Star* [Online]. Available from: https://www.expressandstar.com/news/health/coronavirus-covid19/2020/04/08/two-coronavirus-hate-crimes-a-week-reported-to-police/ [All accessed 16.4.20].

61 MedConfidential. (2020). Apps for the next pandemic. *Medconfidential.org*. Available from: https://medconfidential.org/2020/apps-for-the-next-pandemic [Accessed 16.4.20].

Immunoprivilege – lessons from the 19th-century Deep South
Excerpted from Kathryn Olivarius, 'The Dangerous History of Immunoprivilege', The New York Times, 12 April 2020

Yellow fever, a mosquito-borne flavivirus, was inescapable in the 19th-century Deep South and a point of near-constant terror in New Orleans, the region's hub. In the six decades between the Louisiana Purchase and the Civil War, New Orleans experienced 22 full-blown epidemics, cumulatively killing over 150,000 people. (Perhaps another 150,000 died in nearby American cities.) The virus killed about half of all those it infected and it killed them horribly, with many victims vomiting thick black blood, the consistency and color of coffee grounds. The lucky survivors became "acclimated," or immune for life.

Antebellum New Orleans was a slave society where whites dominated free people of color and enslaved people through legally sanctioned violence. But another invisible hierarchy came to co-mingle with the racial order; white "acclimated citizens" stood atop the social pyramid, followed by white "unacclimated strangers," followed by everyone else. Surviving yellow fever was locally known as the "baptism of citizenship:" proof that a white person had been chosen by God and had established himself as a legitimate and permanent player in the Cotton Kingdom.

Immunity mattered. "Unacclimated" white people were considered unemployable. As the German immigrant Gustav Dresel lamented in the 1830s, "I looked around in vain for a position as bookkeeper," but "to engage a young man who was not acclimated would be a bad speculation." Life insurers rejected unacclimated applicants outright or else charged a hefty "climate premium." If you were white, immunity-status impacted where you lived, how much you earned, your ability to get credit, and whom you were able to marry. It's no wonder, then, that many new immigrants actively sought sickness: huddling together in cramped dwellings, or jumping into a bed where friends had just died — the antebellum forerunners to "chickenpox parties," except much deadlier.

4. Fraud and abuse

Malicious individuals will want to profit from immunity certification. Simple examples include extorting individuals and organisations through threats of falsifying data, selling services by pretending that a workforce is immune when they are not, or helping individuals to falsify their own immunity status. Some activities for organised crime are curtailed by the virus, meaning that there is both motivation and capacity to respond to new opportunities.[62]

5. Perverse incentives

There will be incentives for people to try to create incorrect results. An individual may want to show that they are immune when they are not, so that they can leave a house where they have been isolating for several weeks, or to get a job so that they can buy food. Other individuals may want to claim that they are not immune when they are, perhaps so that they do not need to do work that they think is dangerous, or so that they can claim welfare benefits. These incentives will be affected by other factors: government welfare policies and employment protections will affect people's need to seek employment, organisation's employment policies and national immigration rules will affect people's need to be immune to find work or visit family[63]. While many of these incentives can be understood, and mitigated, in a design phase for immunity certification some will only emerge when it is implemented.

Recommendations

Finding: There is broad agreement that widespread testing is the only route through which the UK can exit the coronavirus crisis. Immunity testing is likely to be a key part of this strategy. However, there does not yet seem to be a robust scientific means of testing immunity. As such, there is no credible basis for establishing a comprehensive regime of immunity certification at this time.

Recommendation: Until a robust and credible means of immunity testing is developed, Government should focus on developing a comprehensive strategy to establish how immunity testing will be conducted, how immunity will be certified, and how immunity certification will be integrated into policy and processes including those pertaining to travel, movement, work and schooling. The strategy should be made public and open to public scrutiny.

62 Global Initiative Against Transnational Organised Crime. (2020). Crime and contagion: the impact of a pandemic on organised crime. *Globalinitiative.net*. Available from: https://globalinitiative.net/wp-content/uploads/2020/03/CovidPB1rev.04.04.v1.pdf [Accessed 16.4.20].

63 Dharwadker, S. (2020). Travel after COVID-19. *Keesing Platform*. Available from: https://platform.keesingtechnologies.com/travel-coronavirus/ [Accessed 16.4.20].

Finding: The establishment of a regime for immunity certification will have deep societal implications. It may lead to arbitrary and unfair restrictions on individuals' access to transport, services, employment, movement and other rights and freedoms on the basis of their immunity status. Discrimination and stigmatisation may become commonplace if immunity becomes an integral element of an individual's identity as we transition from the crisis. The public will need to trust and support any government strategy that centres on immunity certification.

Recommendation: Government strategy must clearly define the role that immunity certification will play during transition and beyond the crisis. It must be clear to the public what values are being prioritised and traded-off in a transition strategy that centres on immunity certification.

Government should advance primary legislation specifying when, why and under what conditions individuals are required to be tested for and disclose their immunity status. This legislation should prevent private and public actors from requesting or requiring disclosure of immunity status outside of defined circumstances. Parliament must ensure such legislation is subject to robust and expert debate and scrutiny.

Finding: Should an immunity certification regime be determined necessary, a secure digital system based on open standards may be an effective way of maximising benefits while minimising fraud and abuse. However, it would need to be bolstered by non-digital methods in order to account for digital exclusion and prevent further harm to vulnerable groups.

Recommendation: Government must establish an independent Group of Advisors on Technology in Emergencies to oversee the development and testing of any prospective digital immunity certification system. The Group of Advisors should be charged with stipulating privacy-preserving measures that the system should integrate, and measures for ensuring vulnerable groups are not excluded from the operation of the system.

About this report

This report was authored by the Ada Lovelace Institute, with the assistance of Peter Wells. It is based on the input and advice of a range of experts who provided direct input, some of whom attended a virtual meeting on Tuesday 7 April 2020:

Tariq Khokhar, Head of Data for Science and Health, Wellcome Trust
Professor Dave Archard, Emeritus Professor, Queen's University Belfast
Professor Lilian Edwards, Chair of Law, Innovation and Society, Newcastle Law School
Dr Marion Oswald, Vice-Chancellor's Senior Fellow in Law at the University of Northumbria
Dr Edgar Whitley, Associate Professor of Information Systems, London School of Economics (LSE)
Dr Alison Powell, Director of the JUST AI Network, LSE
Dr Lina Dencik, Director of the Data Justice Lab, Cardiff University
Professor Pete Fussey, Research Director for the Human Rights, Big Data and Technology Project, University of Essex
Helen Mountfield QC, Principal, Mansfield College
Professor Susan Michie, Director of UCL Centre for Behaviour Change
Jeni Tennison, CEO, Open Data Institute
Rachel Coldicutt
Dr Michael Veale, Lecturer in Digital Rights and Regulation, UCL
Dr Seeta Peña Gangadharan, Assistant Professor, Department of Media and Communications, LSE
Orla Lynskey, Associate Professor of Law, LSE
Renate Samson, Senior Policy Advisor, Open Data Institute
Dr Nina Putnis, NHS
Ravi Naik, Director, AWO

The content and conclusions of this review are not directly endorsed by the experts.

About the Ada Lovelace Institute

The Ada Lovelace Institute was established by the Nuffield Foundation in early 2018, in collaboration with the Alan Turing Institute, the Royal Society, the British Academy, the Royal Statistical Society, the Wellcome Trust, Luminate, techUK and the Nuffield Council on Bioethics.

The mission of the Ada Lovelace Institute is to ensure that data and AI work for people and society. We believe that a world where data and AI work for people and society is a world in which the opportunities, benefits and privileges generated by data and AI are justly and equitably distributed and experienced.

We recognise the power asymmetries that exist in ethical and legal debates around the development of data-driven technologies, and will represent people in those conversations. We focus not on the types of technologies we want to build, but on the types of societies we want to build.

Through research, policy and practice, we aim to ensure that the transformative power of data and AI is used and harnessed in ways that maximise social wellbeing and put technology at the service of humanity.

We are funded by the Nuffield Foundation, an independent charitable trust with a mission to advance social well-being. The Foundation funds research that informs social policy, primarily in education, welfare and justice. It also provides opportunities for young people to develop skills and confidence in STEM and research. In addition to the Ada Lovelace Institute, the Foundation is also the founder and co-funder of the Nuffield Council on Bioethics and the Nuffield Family Justice Observatory.

adalovelaceinstitute.org
@AdaLovelaceInst
hello@adalovelaceinstitute.org

Ada Lovelace Institute
28 Bedford Square
London WC1B 3JS
+44 (0) 20 7631 0566

Registered charity 206601

Design: williamjoseph.co.uk