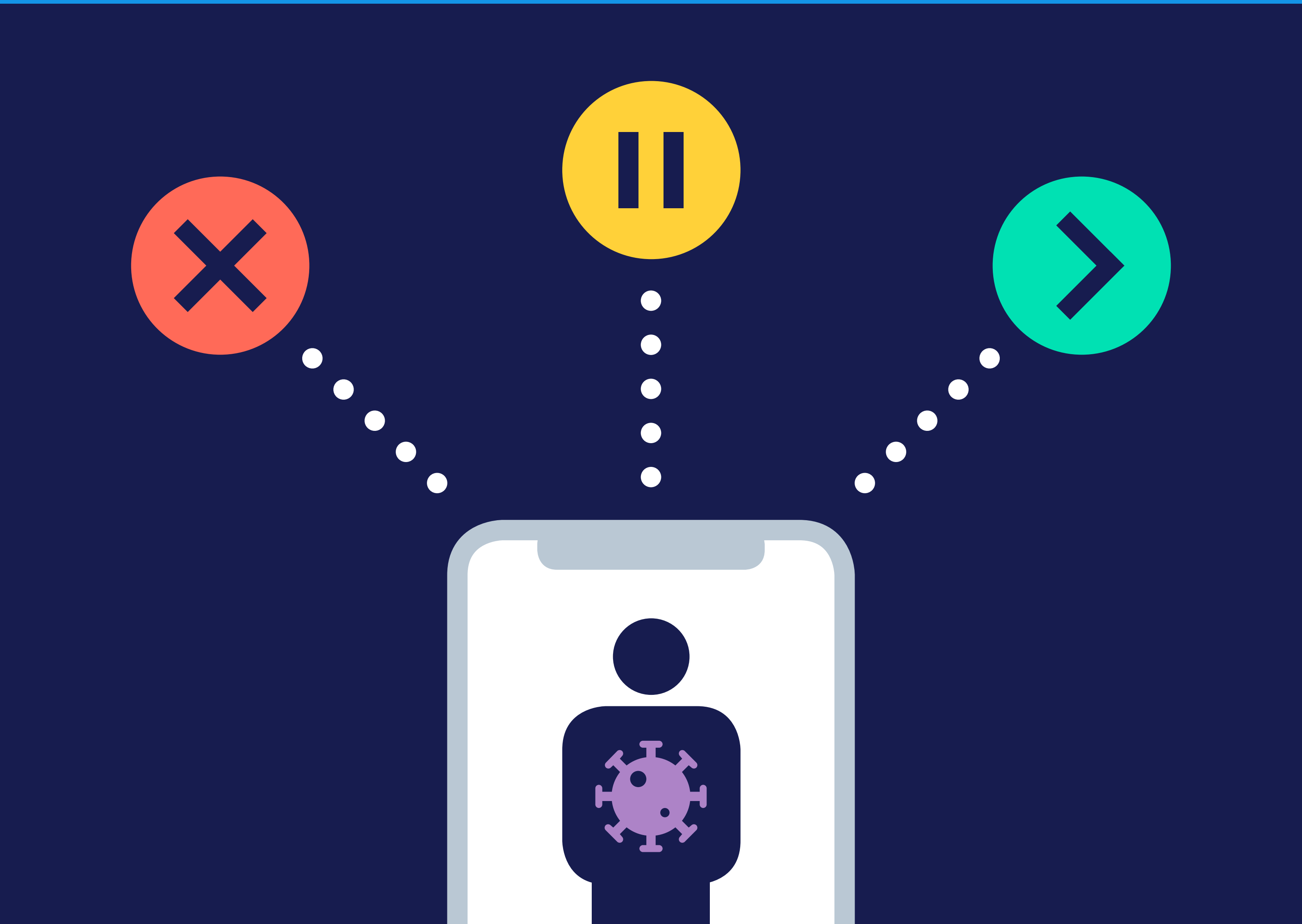
Ada Lovelace Institute

No green lights, no red lines

Public perspectives on COVID-19 technologies

July 2020



How to contain the COVID-19 virus swiftly and effectively, with minimum impact on health, economies, societies and individuals, is the defining question of 2020.

As lockdown eases after the first wave, we are at a moment when Government and policymakers can consider how to balance risk and shape freedoms at a local, or even individual, level. Novel and intrusive technologies are likely to play a part in that, but – as we have seen with contact tracing – it will be a challenge to navigate the risks and trade-offs.

In this report, we articulate lessons from public engagement to assist Government and policymakers navigating difficult dilemmas when deploying data-driven technologies to manage the pandemic, and when judging what risks are acceptable to incur for the sake of greater public health.

There are no clear green lights or neat red lines here, so these nuanced learnings must be applied to the future measures to contain the virus, protect and preserve society, and save lives.

Contents

Summary

Data-driven tools and systems are being developed and tested for use in response to multiple challenges presented by COVID-19. COVID apps under consideration by Government include contact tracing apps, immunity certification and digital health status apps.

Technology could play a powerful role in supporting public health strategy, but using novel technologies to undertake a form of public monitoring or the creation of a form of public health monitoring will be controversial, and raises complex social issues. Contemplating their deployment is only justifiable in the face of – and for the duration of – a grave crisis.

Given the complexity and importance of these tools, they must be developed with public legitimacy for two reasons. First, COVID-19 technologies will only be effective if they are adopted and adhered to by the public. That requires technical tools and policy architecture surrounding their use to be seen as acceptable and proportionate solutions.

Second – and perhaps more importantly – future apps may be vital to manage this health crisis or future crises. Getting COVID-19 technologies wrong now may block essential options for future technical solutions or, worse, undermine faith in public health strategies.

To support technology developers and policymakers to design tools that anticipate the preferences and mitigate the legitimate concerns of the public, we have pulled relevant insights from three public deliberation projects, identifying six lessons that should be brought to bear on the design and deployment of COVID-19 technologies:

1

Trust isn't just about data or privacy. To be trusted, technology needs to effective and be seen to solve the problem it is seeking to address.

2

People's experiences and expressions of identity matter – and are complex. Categorising individuals can be reductive and disempowering.

3

Public health monitoring and identity systems are seen as high-stakes applications that will need to be justified as appropriate and necessary to be adopted.

4

Tools must proactively protect against errors, harms and discrimination, with legitimate fears about prejudice addressed directly.

5

Apps will be judged as part of the system they are embedded into – the whole system must be trustworthy, not just the data or the technology.

6

The technologies under discussion are not viewed as neutral. They must be conceived and designed to account for their social and political nature.

These lessons from the public offer neither clear green lights nor neat red lines, but developing and deploying new technologies is not neat or easy, especially in a crisis.

It is clear from the nuance and consideration expressed by these informed publics, organised in this report, that citizens have the capacity to weigh these challenging issues.

Politicians, policymakers and technology developers will benefit by designing apps that consider the preferences and legitimate concerns of members of the public detailed here.

To create systems that work for the public, these challenges and concerns need to be acknowledged and explored, rather than discounted and silenced, and complexities must be designed in.

Introduction

The COVID-19 pandemic has opened the door to the development and deployment of public health monitoring technologies, like contact tracing apps and immunity certificates. Meaningfully engaging the public in their development, and understanding their perspectives, is vital to ensure successful roll-out.

These technologies may become components of both the pandemic response and of emerging public health identity systems (PHIs) for verifiably sharing private health-related data.[1] These applications raise urgent questions around social and political issues like identity, surveillance, citizenship, discrimination, and broader considerations about the role of identity technologies in society.[2]

Due to the rapid pace of these developments – propelled by the urgent health need to respond to COVID-19 and the consequent political will to adopt these tools – public debate on these issues is critical.[3]

Recent polling has suggested that the UK public *would* accept greater use of technologies like digital contact tracing or health status reporting to tackle the pandemic.[4] However, attitudes expressed in polls do not translate into behaviour, and surveys cannot always capture deeper concerns and challenges – such as the standards required to build trust or the consequences of a perverse incentive to gain 'immune' status by purposely becoming infected.

[1] Ada Lovelace Institute (2020) *A public health identity? Health status apps, immunity certificates and biometrics*. Available at: https://www.adalovelaceinstitute.org/our-work/identities-liberties/a-public-health-identity-health-status-apps-immunity-certificates-and-biometrics/ (Accessed: 29 June 2020).

[2] Nuffield Council on Bioethics (2020) *New briefing: COVID-19 antibody testing and 'immunity certification'*. Available at: https://www.nuffieldbioethics.org/news/new-briefing-covid-19-antibody-testing-and-immunity-certification (Accessed: 29 June 2020).

[3] *Biometrics Commissioner's address to the Westminster Forum: 5 May 2020* (2020) GOV.UK. Available at: https://www.gov.uk/government/speeches/biometrics-commissioners-address-to-the-westminster-forum-5-may-2020 (Accessed: 29 June 2020).

[4] Taylor, E. et al. (2020) *Coronavirus: survey reveals what the public wants from a contact-tracing app, The Conversation*. Available at: https://theconversation.com/coronavirus-survey-reveals-what-the-public-wants-from-a-contact-tracing-app-138574 (Accessed: 29 June 2020).

What are public health identity systems?

'Public health identity' (PHI) systems share verified, private health data for public health purposes. They bring personal health data into the public sphere.

These systems can be used to share raw data on health testing and other metrics. They may also generate a pass/fail certification or a dynamic, personalised risk score based on that data. Some PHI systems may link data to an individual by using a form of biometric identification.

PHIs will categorise individuals according to health metrics, or risk of COVID-19 infection or transmission, and use those categories to 'stream' society.

Streaming would determine people's access to employment, mobility, travel, and social interaction, and allow or deny access to different kinds of public and private spaces, like cafés or airports, based on an individual's health status, and may rely on biometric technologies or digital surveillance tools.

PHI systems under consideration include health status apps and 'digital immunity certificates'. The data-driven technologies underpinning these systems allow for iterative increases in scope towards a comprehensive 'digital identity'.

The support and acceptance many people may express in the use of these systems contains nuance and expectations for oversight, limitations and other safeguards. Moreover, as trials of the UK contact tracing app[5] and muted success of other apps around the world[6] have shown, failing to engage with the public can lead to vital gaps in understanding of what determines the successful roll-out of a data-driven health tool.

To help address these gaps, deeper engagement with informed publics is needed. Understanding public perspectives will assist Government, technology developers and policymakers as they navigate difficult trade-offs when deploying data-driven and digital tools to manage the pandemic. The lessons from this must be applied to current and future measures to contain the virus, protect and preserve society, and save lives.

> **'I am a bit fearful that we are sleepwalking into certain things as a society.'**
>
> **Participant in the Citizens' Biometrics Council, Bristol, February 2020**

[5] Burgess, M. (2020) 'Why the NHS Covid-19 contact tracing app failed', *Wired UK*, 19 June. Available at: https://www.wired.co.uk/article/nhs-tracing-app-scrapped-apple-google-uk (Accessed: 29 June 2020).

[6] Abboud, L. and Miller, J. (2020) 'French give cool reception to Covid-19 contact-tracing app', *Financial Times*. Available at: https://www.ft.com/content/255567d5-b7ec-4fbe-b8a9-833b3a23f665 (Accessed: 29 June 2020).

Method: drawing on public engagement to inform the debate

At the Ada Lovelace Institute, convening diverse voices and fostering informed public debate are central to our work ensuring data and AI work for people and society. Before the COVID-19 pandemic, we had established a citizens' council to understand public perspective on identity technologies, and during the pandemic we convened a rapid online deliberation on the role of technology in the UK Government's response to COVID-19.

To inform the debate around PHIs, we have drawn insights from these recent projects:

1. **The Citizens' Biometrics Council:** In February 2020, we convened 60 members of the public to form the Citizens Biometrics Council, to consider evidence and deliberate on the use of biometrics technologies.[7] The Council held its first workshops before the UK had any cases of COVID-19. Lockdown came into effect halfway through the process, and we have paused the Council until we can reconvene safely.

2. **Community Voices Workshops:** To ensure marginalised voices were heard in the Council's biometrics debate, we ran Community Voice workshops with three groups of 10–15 people: Black, Asian and Ethnic Minorities; people who are disabled; and the LGBTQI community. These groups were identified as among those who faced disproportionate impacts from biometrics technologies.

   These workshops informed our work on biometrics and are feeding into the Citizens' Biometrics Councils' findings. We have also drawn perspectives from these workshops on how technology and structural inequality and injustice interact.[8] We also paused this process when lockdown came into effect.

[7] Ada Lovelace Institute (2019) *Citizens' Biometrics Council*. Available at: https://www.adalovelaceinstitute.org/our-work/identities-liberties/citizens-biometrics-council/ (Accessed: 29 June 2020).

[8] Ada Lovelace Institute (2020) *Making visible the invisible: what public engagement uncovers about privilege and power in data systems*. Available at: https://www.adalovelaceinstitute.org/making-visible-the-invisible-what-public-engagement-uncovers-about-privilege-and-power-in-data-systems/ (Accessed: 29 June 2020).

3. **Online deliberation on technology use in the UK response to COVID-19:** In May 2020, 25 members of the public took part in a series of online deliberation workshops during a three-week period. Participants considered the role of technology in the UK Government's response to COVID-19 and produced a set of values to guide the development of future COVID-related technologies. They formed and shared expectations and concerns about the NHSX digital contact tracing app and emerging concepts surrounding immunity certification.

From the three deliberation processes, we gained important insights into the issues raised by the data-driven technologies that may be used in public health monitoring and PHIs.

That the Citizens' Biometrics Council projects were already deliberating on these issues is timely, but the deliberation so far reflects only a part of this process – the topics, themes and concerns that emerged as Council members grappled with issues of technological surveillance, public safety, algorithmic bias and more.

The findings here are therefore not conclusions of extensive deliberation but rather reflective of the concerns, challenges and considerations for the development of PHIs. These are not direct recommendations but indications of the temperature of public opinion.

Across all three public convenings, the insights shared represent perspectives from before and during the COVID-19 pandemic. We are still in the middle of this crisis and must recognise that attitudes are continually shifting as the situation unfolds.

We can't and don't attempt to use these processes to predict where they will settle beyond the end of the pandemic.

Each project has its own aims and outputs in addition to this report.

What is public deliberation?

Traditional forms of public research like attitudes polling can offer indications about opinions and current understanding, and public polling around acceptability and trust has shaped the UK Government's view of their options around COVID-19 technologies. However, more in-depth public deliberation enables a richer understanding of societal impacts, limits, trade-offs and pitfalls.

Research processes that inform participants, enable them to offer more nuanced views and reach consensus following debate and evidence are time consuming. But these processes deliver value, using experts and moderators to foster mutual understanding between researchers, developers, policymakers and those affected by technologies by guiding small groups of individuals through controversial scenarios including dilemmas and trade-offs.

At moments of crisis, where it is critical that tools are developed with public legitimacy, it can be difficult to convene a deliberative process that is able to keep ahead of policy decisions and technical innovation.
But deeper understanding of people's perspectives, beyond attitudes polling, is crucial to address the challenges these technologies pose and understand what the public expect for their proportionate, responsible and trustworthy use.

Emerging insights: public perspectives on technologies that monitor people and health

Emerging from the three deliberation projects we saw a set of values, concerns and perspectives about public health identity systems that can help to inform the debate going forward.

We highlight five themes specifically, and although discussed separately, these topics are intertwined and must be addressed cohesively by policymakers and those responsible for developing and deploying new technologies during the pandemic.

1. Identity

People's understandings and experiences of 'identity' are complex. The concept holds multiple meanings and conceptions for different individuals, and all-too-often a person or group's expression of their own identity contrasts with categorised identities imposed on them by society and embedded in systems.

Many technologies and systems can only capture an individual's sex or gender as 'male' or 'female' for example, drawing on reductive stereotypes and ignoring a wide spectrum of expressed gender identities.

Participants expressed how systems that categorise citizenship or identity often entrench antiquated notions of 'belonging' by defining which identity characteristics are legible or accepted. This way of seeing identities does not reflect modern intersections of individuality, nationality, community and ethnicity.

Identity and its politics are much-studied fields of research.[9] Systems (technological or administrative) that impose identity onto others and reduce complex experiences of identity to reductive, binary categories are not only inaccurate: they are disempowering.

[9] See, for example: Young, Iris Marion (1990) *Justice and the Politics of Difference*, Princeton: Princeton University Press, or: Combahee River Collective (1982) 'A Black Feminist Statement', in *All the Women are White, All the Blacks are Men, But Some of Us Are Brave: Black Women's Studies*, Gloria T. Hull, Patricia Bell Scott, and Barbara Smith (eds), New York: Feminist Press.

> **‘If there’s a CCTV camera, you’re less likely to act outside of what’s acceptable, because you’re under observation. So you modify your own behaviour, you stop being as wild, or as wonderful, or as kinky, or as strange, or as bizarre, as beautiful as you could possibly be [...] And no-one has asked us if we want to live in that society.’**
> Citizen from Brighton Community Voice workshop, December 2019

Participants shared concerns that once labelled by a biometric or identity system no other aspects of an individual’s identity will be given equal consideration. Labels like gender, age and ethnicity were commonly cited among those which can be poorly categorised by systems.

In public health identity systems, labels like ‘immune’ or ‘not-immune’ may obscure other important aspects of an individual’s identity, including other health conditions.

Participants across these engagements expressed that they want and deserve the right to express their identity freely. They are concerned that technological identity systems put people in pre-defined ‘boxes’ that remove control or freedom to define and express their own identity. These systems must not erode individuals’ and communities’ control over identities or threaten to establish static categories as the primary means through which people are seen, recognised or known.

2. Accuracy

Many participants shared concerns about the accuracy of biometric and identity technologies. Evidence that facial recognition systems aren’t equally effective across gender and skin-tone[10] was considered seriously, as well as low accuracy during actual deployment of biometric systems[11] or when algorithms fail.

The consequences of these inaccuracies – from lack of effectiveness through to severe discrimination – were commonly regarded as unacceptable. Many people articulated a minimum standard of 100% accuracy, and acknowledged the important role of safeguards like humans in-the-loop.

Accuracy has been framed as a red herring by technologists, who subscribe to a model of systems designed and deployed with rigorous testing and iterative development to consistently become more effective and precise. However, these technicalities were not the focus of people’s concerns.

[10] Buolamwini, J. et al. (2018) *Gender Shades*. Available at: http://gendershades.org/overview.html (Accessed: 29 June 2020).

[11] Fussey, P. and Murray, D. (2019) *Independent Report on the London Metropolitan Police Service’s Trial of Live Facial Recognition Technology*. University of Essex Human Rights Centre. Available at: http://repository.essex.ac.uk/24946/ (Accessed: 29 June 2020).

> **‘I guess I’m of the age, where I think that the combination of human and technology is going to be safer, stronger, more resilient and robust, than either one or the other.’**
> **Participant in the Citizens’ Biometrics Council, Bristol, February 2020**

> **‘It was said that no system is 100% secure, [but] we’re in such a crisis and we’re so behind tracking that we really need to give this a try.’**
> **Participant in online deliberation, May 2020**

The citizens’ discussions of accuracy centred less on the technology’s function and more about its outcomes. Does *the use* of a biometric or identity system lead to errors that negatively affect individuals? If so, this is unacceptable, regardless of whether the error is the fault of poor technology, biased human values in the development of the technology, or flaws in the infrastructure in which the technology is deployed.

For COVID-19 related technologies, we could conclude that errors which lead to negative outcomes for individuals – whether health or economic – would be unacceptable. But some expressed the need for a trade-off between reducing errors and the urgency of tackling the pandemic.

In the online deliberation in May, while almost all participants expressed concerns about tools like digital contact tracing apps, many concluded they would still use one if it helped to tackle the pandemic and save lives.

Deploying digital tools need not be an either/or scenario, however. Building robust processes around technologies can help to mitigate risks of unfairness. For instance, consider a situation where someone is wrongly prevented from accessing a service because of a technological error that suggests they have COVID-19 when they don’t. Rather than not deploying a system because of errors, individuals must have the right to challenge decisions made by public health identity systems, the opportunity to correct data held in those systems, and safeguards must be in place to amend errors and prevent people from being disadvantaged by inaccuracy.

3. Discrimination and accessibility

Intertwined with identity and accuracy is the concern that these technologies affect people in unequal ways. Systems that aren’t consistently accurate across characteristics like skin tone or gender can lead to discrimination, which participants found unacceptable. But thinking about perfectly accurate technologies also raised concerns, especially about the possibility of targeting disadvantaged or vulnerable groups, like immigrants or the homeless. There was anxiety that biometric technologies could be used to target religious minorities[12] or individuals from LGBTQI groups.

[12] Mozur, P. (2019) ‘One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority’, *The New York Times*. Available at: https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html (Accessed: 29 June 2020).

As well as discrimination against certain groups, participants raised questions around accessibility and inclusion. Not everyone is able to access or use a technology equally, particularly where health-related or biometric characteristics are involved, such as with fingerprint, voice or facial recognition technology.[13] Some individuals' voices, fingerprints and other physical attributes might change in ways that biometrics technologies cannot account for. Those who are digitally excluded could be left behind too, as they don't have access to or literacy about devices needed to engage with certain systems (e.g. smartphones).

While recognising the positive potential that biometrics technologies can have for accessibility – like voice assistant software for those with reduced sight – the participants warned strongly against becoming systemically reliant on technologies that discriminate and prevent certain members of society from engaging or accessing services.

Discrimination and inclusion are distinct topics, and are brought together deliberately in this analysis to reflect the strong concern among citizens that technologies do not affect everyone equally. Some are less able to engage and enjoy benefits, while others disproportionately face burdens or challenges because of biases in design and deployment.

Where these technologies are used to tackle COVID-19 – which affects everyone significantly but not equally[14] – the risks of excluding those most vulnerable or creating new tiers of discrimination and stratification are not ones that society can afford.[15]

> **'Apps like Google Home and Siri don't always work if you have a speech impairment, etc. This is another challenge – are we going to be maintaining appropriate and accessible services for people? Are there going to be people who cannot access all of these things?'**
>
> **Citizen from the Manchester Community Voice workshop, January 2020**

[13] Blanco-Gonzalo, R. et al. (2018) 'Biometrics: Accessibility challenge or opportunity?', *PLOS ONE*. Edited by S. Bakshi, 13(3), https://doi.org/10.1371/journal.pone.0194111

[14] Bibby, J., Everest, G. and Abbs, I. (2020) *Will COVID-19 be a watershed moment for health inequalities?*, The Health Foundation. Available at: https://www.health.org.uk/publications/long-reads/will-covid-19-be-a-watershed-moment-for-health-inequalities (Accessed: 29 June 2020).

[15] Bryant, M. (2020) '"Are you immune?" The new class system that could shape the Covid-19 world', *The Guardian*. Available at: https://www.theguardian.com/us-news/2020/jun/10/are-you-immune-the-new-class-system-that-could-shape-the-covid-19-world (Accessed: 29 June 2020).

4. Effectiveness and proportionality

Participants in all our projects often raised questions around whether identity technologies work effectively and whether their use is proportionate. Similarly to the analysis of concerns around accuracy, proponents of these technologies may claim that if they aren't effective, they won't be deployed.

However, people who had first-hand experience of ineffective technologies disputed this view as applicable to laboratory conditions but not the real world. They shared experiences where data about them was wrong, or where a largely automated system couldn't account for a unique or anomalous case.

Many participants in the online deliberation asked whether there was sufficient evidence for the efficacy of interventions like digital contact tracing, and found the lack of evidence around immunity certification or antibody testing concerning.[16,17] When stakes and risks are high, people want reassurance that systems deployed will work. Already, existing COVID-19 technologies are facing the challenge of working as effectively in the real world as they do in the lab.[18]

Even if effective, some use cases don't feel proportionate to many. The use of biometrics seemed 'heavy handed' to participants when a less-intrusive and as-effective method exists. This was particularly true for low-stakes scenarios where public safety isn't a concern. Using facial recognition for a gym entry system, for example, felt disproportionate when an as-effective non-biometric solution is sufficient, like membership cards.

Because biometrics technologies *feel* more intrusive, the justification for their use must meet higher thresholds (and in the eyes of some participants, often fails to do so). Even when considering technologies deployed to tackle COVID-19, questions were raised around whether a digital system was proportionate or necessary, when a manual system could be as effective or more effective.

Effectiveness and proportionality represent concerns around technological solutionism – the idea that technology can solve human problems. When it comes to a technology that uses sensitive health or biometric information, participants consistently raised two questions: 'What is the problem that's trying to be solved?' And 'Is this technology appropriate, effective and necessary for that problem?' During the pandemic we face urgent questions, and the answers we choose may have long-reaching effects for our societies.

[16] World Health Organisation (2020) *'Immunity passports' in the context of COVID-19*. Available at: https://www.who.int/news-room/commentaries/detail/immunity-passports-in-the-context-of-covid-19 (Accessed: 29 June 2020).

[17] Mundasad, S. (2020) 'Covid-19 antibody test lacks "proper assessment"', *BBC News*. Available at: https://www.bbc.com/news/health-53169618 (Accessed: 29 June 2020).

[18] Ball, J. (2020) 'The UK's contact tracing app fiasco is a master class in mismanagement', *MIT Technology Review*. Available at: https://www.technologyreview.com/2020/06/19/1004190/uk-covid-contact-tracing-app-fiasco/ (Accessed: 29 June 2020).

5. Trust in the system

> **'I've got no more trust in this than I would in a small-town horoscope or a crystal ball, to be honest.'**
> **Participant in the Citizens' Biometrics Council, Bristol, February 2020**

Public trust is essential for any technological system that is deployed widely and with significant impacts across society. For interventions like digital contact tracing or immunity certification, which require broad uptake and compliance from members of the public to be successful, this is a particular concern for policymakers. More fundamentally however, the participants expressed that they felt the public deserve the *right* to be able to trust such systems, because they will need to comply with them and because of the significant societal impact they may have.

Transparency, accountability, independent oversight and appropriate data protection are key among aspects that members of the public – as well as many technology ethicists and legal scholars[19] – consider vital for trustworthy design, development and deployment of any technological system. In addition to these, measures to limit 'scope creep' are especially vital for PHI systems, as discussed in our rapid evidence review, *Exit through the app store?*[20]

However, when discussing trust, many members of the public veered away from specific technologies and instead spoke about the social and political systems in which they are deployed. For PHIs, those involved in deploying a technology (Government, NHS, private companies and other actors), as well as members of the public using the app, employers and bodies like law enforcement and regulators, are all part of this system. Their actions and public perceptions of those actions make a difference. When trust in one is diminished, the whole system becomes less trustworthy, and even the most perfectly designed technology will be difficult to trust.

The UK Government response to COVID-19 and the murder of George Floyd were topics that participants of our online deliberations reflected on greatly when considering what makes technology trustworthy. Trust is hard won and easily lost. It is lost when systemic injustice and racism lead to discrimination and inequality. It is also lost when those ultimately seen as responsible do not act in a trustworthy manner, regardless of whether that relates directly to a technology or not.

> **'I don't understand how the population is going to download and trust an app when they don't even listen or trust the government and adhere to the rules of lockdown?'**
> **Participant in online deliberation, May 2020**

[19] OECD (2019) 'Forty-two countries adopt new OECD Principles on Artificial Intelligence'. Available at: https://www.oecd.org/science/forty-two-countries-adopt-new-oecd-principles-on-artificial-intelligence.htm (Accessed: 29 June 2020).

[20] Ada Lovelace Institute (2020) *Exit through the App Store? Should the UK Government use technology to transition from the COVID-19 global public health crisis*. Available at: https://www.adalovelaceinstitute.org/exit-through-the-app-store-how-the-uk-government-should-use-technology-to-transition-from-the-covid-19-global-public-health-crisis/ (Accessed: 29 June 2020).

Considerations for policymakers and technology developers

The concerns raised through public deliberation show that there is no green light for public health identity systems. However, nor are there clear red lines around what may or may not be acceptable. Balancing the urgent need to address the pandemic with the potential risks and harms new technologies may create is a major challenge, and drawing from public perspectives is crucial to getting it right.

These insights make clear a number of considerations for public health identity systems, which are clear lessons that policymakers and technology developers must take on board:

1

Trust isn't just about data or privacy. Technology must also be effective and seen to solve the problem it seeks to address.

A prime concern for the public is that any technology deployed during this crisis is effective at solving the problems faced by individuals and wider society.

Technological interventions must be grounded in robust evidence and shown to be effective through rigorous monitoring and evaluation.

2

People's experiences and expressions of identity matter – and are complex. Categorising individuals can be reductive and disempowering.

There is anxiety about the creation of technological identity systems that put people in pre-defined boxes or establish static categories as the primary means through which people are seen, recognised or known.

Systems must be deployed in ways that foster solidarity, equity and inclusion, rather than allowing the risk that categorisation creates opportunities for discrimination, injustice and exclusion.

3

Public health monitoring and identity systems are seen as high-stakes applications that will need to be justified as appropriate and necessary to be adopted.

The idea of proportionality (while not expressed with the use of that term) runs deep in public consciousness. It is expressed in the sentiment that the right to consent to or opt out of the use of identity systems, and clear justifications and guidelines for use, are crucial to the trustworthy development of PHI and health monitoring systems.

Identity systems and health monitoring tools must be deployed only if they can be justified as appropriate and necessary.

4

Tools must proactively protect against errors, harms and discrimination, with legitimate fears about prejudice addressed directly.

Many people's experiences suggest that negative impacts from discrimination are a consequence of identification or categorisation systems, and there are legitimate fears that widespread checking of people's health status may open up new possibilities for prejudice.

It is unlikely that an entire PHI system (from testing, through data infrastructure and algorithms, to outcomes) will be completely faultless and free from errors that could exclude people, create difficulties for individuals and discriminate.

Appropriate provisions, such as well-trained humans-in-the-loop, and meaningful opportunities for individuals to contest incorrect outcomes must be embedded across these systems.

5

Apps will be judged as part of the system they are embedded into – the whole system must be trustworthy, not just the data or the technology.

Technology is part of a social and political system, made up of those responsible for developing and deploying it and those who use it, as well as the technological components of hardware and code. When reflecting on what makes a digital tool trustworthy, people are acutely aware that the trustworthiness of the entire system is central to the trustworthiness of the technology itself.

6

The technologies under discussion are not viewed as neutral; they must be conceived and designed to account for their social and political nature.

Informed citizens do not consider technology and its impacts as separate from society or politics. Technology cannot be decoupled or isolated from questions of the nature of the society it will shape, whether solidaristic or individualistic, inclusive or divisive. Technology providers for COVID-19 technologies need to understand they are shifting the social-political fabric of society in a crisis, and potentially beyond a crisis.

Conclusion

The COVID-19 technologies that are developed and implemented now will have a legacy far beyond the end of this pandemic.

How these systems interact with individuals' experiences and expressions of identity, how prone to error they are and how they may contribute to discrimination and exclusion are all key concerns for the public.

What evidence there is for their effectiveness, justification for their proportionate use, and how trustworthy the entire system in which they are deployed are central to whether the public will accept technology and how they'll adopt it.

The Citizens' Biometrics Council will continue to deliberate on digital identity systems to contribute to our collective understanding and articulate what is or is not okay when it comes to the use of biometrics in a post-pandemic world.

At times of crisis, decisions are made, and technologies deployed at rapid pace and on a society-wide scale. Meaningfully engaging with the public not only ensures better decision-making, it also contributes to designing technologies that are proportionate, trustworthy and ultimately more effective.

The Citizens' Biometrics Council and Community Voices workshops are delivered in partnership with Hopkins Van Mil, and will conclude in Autumn 2020. The online deliberation was delivered in partnership with Traverse, Involve and Bang the Table.

Citation
If you are using this document in your own writing, our preferred citation is:

Ada Lovelace Institute (2020) 'No Green Lights, No Red Lines: Public perspectives on COVID-19 technologies'.
Available at: https://www.adalovelaceinstitute.org/no-green-lights-no-red-lines

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

Founded by the Nuffield Foundation
Registered charity 206601

Design: williamjoseph.co.uk