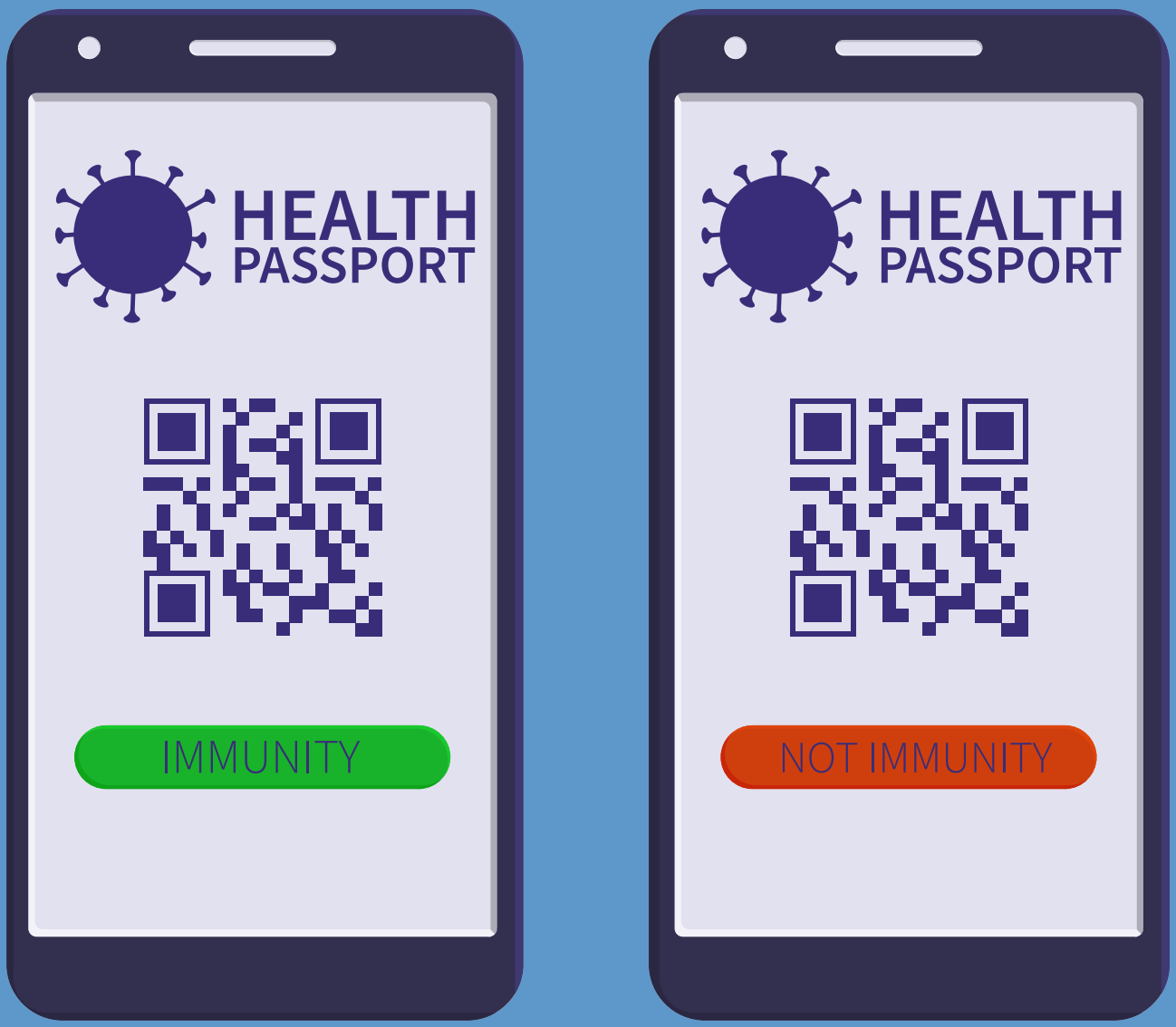
Digital Health Passports for COVID-19:
Data Privacy and Human Rights Law



UNIVERSITY OF EXETER

UKRI Economic and Social Research Council

Contents

Executive Summary

Context of the study

- Digital health passports, sometimes also referred to as 'immunity passports', are digital credentials that, combined with identity verification, allow individuals to prove their health status (such as the results of antigen and antibody tests, and eventually, digital vaccination records).

- Multiple initiatives to develop and deploy digital health passports are currently underway in the UK and abroad, to facilitate the return to work, travel, and live-audience large sports events.

- These initiatives build on existing digital identity technologies and may use, for example, mobile phone applications, QR codes or electronic bracelets.

- Rapid antigen tests for COVID-19 are increasingly offered by private sector providers in the UK and abroad. Results are often managed through digital platforms.

- To date, the scientific community does not have enough clarity about reinfection and immunity to SARS-CoV-2, including 'herd immunity.'

- Vaccine trials have shown promising early results, raising hopes for vaccine availability and widespread vaccination by mid-2021.

Key findings and policy recommendations

- Digital health passports may contribute to the long-term management of the COVID-19 pandemic.
- However, digital health passports pose essential questions for the protection of data privacy and human rights, given that they:
  - use sensitive personal health information;
  - create a new distinction between individuals based on their health status; and
  - can be used to determine the degree of freedoms and rights one may enjoy.
- Measures supporting the deployment of such digital health passports may interfere with the respect and protection of data and human rights, in particular the rights to privacy, equality and non-discrimination, and the freedoms of movement, assembly, and to manifest one's religion or beliefs.
- While public health interests may justify such interferences, policymakers must strike an adequate balance between protecting the rights and freedoms of all individuals and safeguarding public interests when managing the effects of the pandemic.

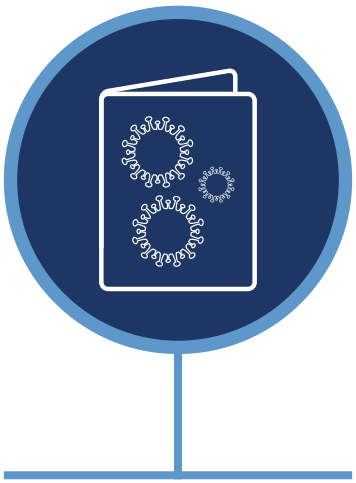
Accordingly, it is recommended that:

1. **Policymakers should require digital health passport providers to adopt appropriate technical and organisational measures and undertake data protection impact assessments to address potential data privacy-invasive situations proactively.**

In doing so, they should take into account not only the potential risks for data privacy but also the situations in which the deployment of digital health passports is likely to result in a high risk to individuals' rights and freedoms.

2. **Policymakers should ensure the availability and affordability of COVID-19 tests and vaccines (once developed) to the whole population before any large-scale deployment of digital health passports.**

Any failure to address the issues of availability and affordability of COVID-19 tests and vaccines risks dramatically excluding already vulnerable populations from protection and may disproportionately restrict the exercise of their legal rights.



Introduction

Digital health passports, sometimes also referred to as 'immunity passports', are digital credentials that, combined with identity verification, allow individuals to prove their health status (such as the results of antigen or antibody tests, or eventually digital vaccination records). They build on existing digital identity technologies and may be deployed via, for example, mobile phone applications, QR codes and electronic bracelets.

Digital health passports may contribute to the long-term management of the COVID-19 pandemic. They could provide for a swift return to 'normal' life without compromising on public health interests.

However, scholars and civil society groups have warned that there are risks associated with these technologies, in particular, with antibody tests used for immunity passports (Ada Lovelace Institute, 2020a; Beduschi, 2020; Gruener, 2020; Kofler & Baylis, 2020; Phelan, 2020; Privacy International, 2020). That is in part because, to date, the scientific community does not have enough clarity about reinfection and immunity to SARS-CoV-2 (Aschwanden, 2020; Iwasaki, 2020; Stephens & McElrath, 2020).

Yet, multiple initiatives to develop digital technologies for health status verification, including immunity and vaccination, are currently underway (COVID-19 Credentials Initiative, 2020; Venkataramakrishnan, 2020).

Policymakers in the UK and abroad have been considering implementing digital health passports as part of their long-term strategy for managing the pandemic (Ada Lovelace Institute, 2020b). Similarly, the World Health Organisation (WHO) and Estonia have recently agreed to jointly develop a digital vaccination certificate that could eventually be used for COVID-19 once a vaccine is available (WHO, 2020a).

Digital health passports could be used to facilitate the return to work, travel, and large gatherings such as large sports events. For instance, two airlines are currently trialling a digital health passport pilot at Heathrow airport, according to which passengers must show their COVID-19 antigen test results on a mobile application before boarding a plane on selected routes (Busby, 2020).

Yet, digital health passports pose essential questions for the protection of data privacy and human rights, given that they (1) use sensitive personal health information, (2) create a new distinction between individuals based on their health status, and (3) can be used to determine the degree to which one may enjoy their rights and freedoms.

The deployment of digital health passports may interfere with an array of fundamental rights, including the right to privacy, the freedoms of movement and peaceful assembly. Therefore, the laws and policies enabling the development and deployment of such digital health passports will have to strike a fair balance between the competing values of safeguarding individual rights and public health interests.

This policy brief draws on independent research on the implications of digital health passports for data privacy and human rights, aiming to:

- Inform decision-makers at an early stage, before large-scale deployment of such digital health passports, about the risks they pose to the protection of these rights.
- Recommend effective strategies for potential risk mitigation.

With that in mind, this policy brief addresses the opportunities and challenges brought about by digital health passports. It summarises the preliminary results following the first phase of the project, which comprised disciplinary and interdisciplinary literature reviews and the evaluation of primary and secondary sources of law.

Using socio-legal methodology (Cownie & Bradney, 2017), the research situates the law within the broader context of using technology and health data in public health emergencies. The socio-legal approach is used to uncover the 'law in context' (as opposed to doctrinal or black-letter law research), to investigate the limits and necessary safeguards imposed by courts when States restrict individuals' human rights.

Research Findings

Assuming that scientific evidence will support the deployment of digital health passports, which is not yet incontrovertibly the case concerning antibody tests, they still pose a variety of questions pertaining to their legal implications.

Since they build on sensitive personal health information to determine the degree of freedom and the rights one may enjoy, the deployment of digital health passports may interfere with the exercise of individuals' legal rights.

It is therefore essential to move beyond the predominant debates about the ethics of health passports (Brown, Kelly, Wilkinson, & Savulescu, 2020; Kofler & Baylis, 2020) and focus on aspects concerning their legal implications for data privacy and human rights law.

Legal framework

In the context of international human rights law, the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic Social and Cultural Rights (ICESCR) are the key international instruments for the protection of human rights.

It is generally accepted that many of the UDHR's provisions have become incorporated into customary international law, which is binding on all States (e.g. Hannum, 1995).

The UDHR laid the foundations of the contemporary protection of human rights. For instance, the UDHR forms the basis of the European Convention on Human Rights (ECHR), which was incorporated in UK law by the Human Rights Act 1998.

The UK ratified the ICCPR and the ICESCR in 1976, but it has not yet incorporated these two international treaties in UK law by a dedicated Act of Parliament.

Data protection is guaranteed by the General Data Protection Regulation (GDPR) as implemented in the UK by the Data Protection Act 2018.

Other relevant statutes under UK law include the Equality Act 2010 and the Disability Discrimination Act 1995. In addition, legislation specific to the coronavirus pandemic is also of interest, including primary and secondary legislation concerning England, Scotland, Wales, and Northern Ireland (The National Archives, 2020).

Data protection and privacy requirements

Article 8 of the ECHR guarantees the respect for one's private life. In the UK, the Human Rights Act 1998 gives effect to this right.

The concept of private life includes the protection of personal information concerning one's health, as well as attributes such as biometric data and DNA samples (S. and Marper v UK; Gaughran v the UK).

State parties to the ECHR, such as the UK, owe treaty obligations to individuals who fall within their jurisdiction (Article 1 ECHR).

No arbitrary interference with privacy rights

Under Article 8 of the ECHR, States must refrain from arbitrarily interfering with one's private life.

As the right to respect for private life is a qualified right, public authorities may be able to justify an interference with this right under specific conditions. Measures restricting the right to privacy must safeguard one of the legitimate aims enumerated in Article 8, paragraph 2 of the ECHR. These include the 'the protection of health' and 'the economic well-being of the country.' In addition, any interference with this right must satisfy the cumulative tests of legality, necessity and proportionality.

The legality test requires that measures interfering with the right to respect for private life must have a basis in domestic law and be compatible with the rule of law (S. and Marper v UK). Therefore, domestic laws providing the legal basis for the deployment of digital health passports must be adequately accessible and foreseeable and afford adequate legal protection against arbitrariness (Malone v UK).

The necessity test demands that the measures adopted address a pressing social need (S. and Marper v UK). The proportionality test requires that the measures taken by public authorities are proportionate to the legitimate aims pursued and entail the least restrictive viable solution (Kennedy v UK; Roman Zakharov v Russia).

In the context of digital health passports, it is possible to argue that there is a vital need to address the unprecedented negative economic and social impact of the COVID-19 pandemic, including the effects of lockdown on people's mental health (O'Connor, et al., 2020). Still, policymakers must be satisfied that there is sufficient scientific evidence to support any large-scale and cross-sector deployment of digital health passports.

Fair balance between competing public and private interests

Member States are also obliged to adopt all measures necessary to ensure that the rights set forth by Article 8 of the ECHR are respected, including in relationships between private parties (Evans v UK; Bărbulescu v. Romania).

In this case, a fair balance must be struck between the competing public and private interests at stake. In striking this balance, States often have a certain margin of appreciation regarding the interests of the community as a whole vis-à-vis the interests of private individuals (Gaskin v UK; Roche v UK).

In the context of digital health passports, they should pay particular attention to the specific protection afforded to health data such as COVID-19 test results.

Health data under the GDPR

Health data, such as the results of COVID-19 tests and eventually, vaccination records, enjoy a reinforced level of protection under Article 9 of the GDPR as implemented in the UK by the Data Protection Act 2018.

Domestic laws must provide adequate and specific measures to safeguard the rights and freedoms of individuals (Article 9-2(i) GDPR) even when pursuing public health interests.

Given that digital health passports contain sensitive personal information, domestic laws and policies should carefully consider the conditions of collection, storage and uses of the data by private sector providers. For instance, providers must comply with the principles of lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality and accountability (Article 5 GDPR).

National data protection authorities—such as the Information Commissioner's Office (ICO) in the UK—have the competence to monitor, investigate and enforce the application of these rules (Articles 57 and 58 GDPR).

Even if individuals consent to have their health data collected, stored and processed for the purposes of using a digital health passport, providers would still need to build data protection into the design of these technologies by default (Article 25-1 GDPR).

For example, digital health passports providers must adopt appropriate technical and organisational measures to address potential data privacy-invasive situations proactively. That includes situations where the processing of the information requires data transfers to third countries for commercial purposes (Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems).

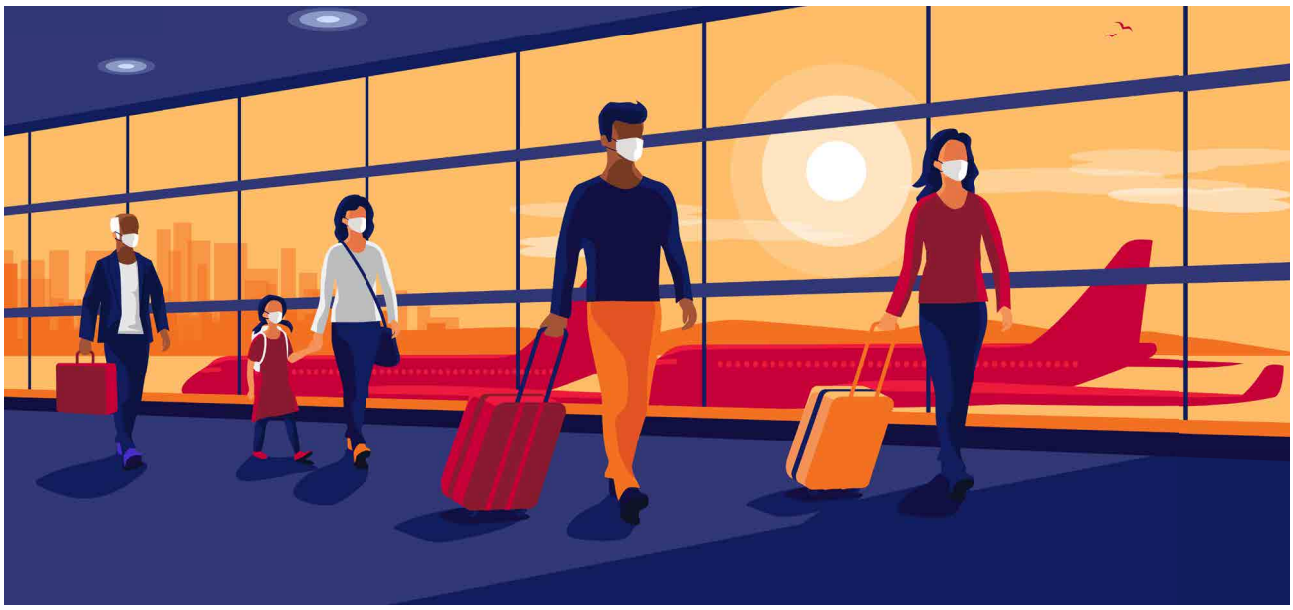
Similarly, domestic laws should require that providers carry out a data protection impact assessment, taking into account that the deployment of digital health passports is likely to result in a high risk to the rights and freedoms of natural persons (Article 35-1 GDPR). Such an assessment of the risks may also inform the evaluation of the necessity and proportionality criteria.

Confidentiality of health data

Confidentiality of health data is a vital principle that has implications beyond the protection of one's privacy, as emphasised by the European Court of Human Rights in a decision about healthcare workers with HIV (I. v Finland).

Research demonstrates that the lack of confidentiality concerning the results of tests for a contagious disease, such as COVID-19, may indeed subject infected individuals to hostility and violence in their communities (McKay, Heisler, Mishor, Catton, & Kloiber, 2020).

Such undesirable outcomes may be compounded by inherent characteristics of those being denied access such as race, ethnicity, gender, or age. Research demonstrates that COVID-19 has already exposed minorities to greater violence and discrimination (United Nations Network on Racial Discrimination and Protection of Minorities, 2020; Public Health England, 2020).



Protection of rights and freedoms

Besides the questions relating to data protection and privacy discussed above, human rights law guarantees an array of legal rights and freedoms that are of relevance for digital health passports. This policy brief discusses the implications that digital health passports have to the freedoms of movement, assembly and to manifest one's religion or beliefs, as well as to the right to equality and non-discrimination.

Freedom of movement, freedom of assembly and freedom to manifest one's religion or beliefs

Freedom of movement has been long recognised as an important right in the common law. The Magna Carta is one of the earliest documents to mention this freedom, then conceptualised as part of every freeman's right to liberty (Magna Carta 1297 Chapter 9 25 Edw 1 cc 1 9 29). English lawyer William Blackstone, in his influential Commentaries of the Laws of England, explained in 1775 that individuals had a right to locomotion in the following terms:

> Next to personal security, the law of England regards, asserts, and preserves the personal liberty of individuals. This personal liberty consists in the power of loco-motion, of changing situation, or removing one's person to whatsoever place one's own inclination may direct; without imprisonment or restraint, unless by due course of law (Blackstone, 1775).

Under contemporary international human rights law, the UDHR recognises the 'right to freedom of movement and residence within the borders of each State' and the 'right to leave any country, including his own, and to return to his country' (Article 13 UDHR).

Article 12, paragraphs 1 and 2 of the ICCPR provide that 'everyone lawfully within the territory of a State shall, within that territory, have the right to liberty of movement and freedom to choose his

residence' and that 'everyone shall be free to leave any country, including his own'. The addition of the term 'lawfully' to the first paragraph reaffirms the right of States to control the entry, residence, and expulsion of foreigners.

Because the UDHR and the ICCPR are not incorporated in UK law, the contours of the freedom of movement in the UK are defined by that which is not prohibited by legislation or common law (Moeckli, 2016, p. 226).

Accordingly, freedom of movement can be subjected to limitations and restrictions, in particular in situations where public authorities are motivated by the interests of the common good (Austin and Others v UK). However, restrictions on freedom of movement may also interfere with the respect for other rights, such as the right to respect for private life (Article 8 ECHR).

Freedom of assembly is protected under Article 11 of the ECHR, which provides that 'everyone has the right to freedom of peaceful assembly'. This is not an absolute right and as such, it can be restricted. Restrictions must pursue at least one of the legitimate aims under the second paragraph of Article 11 of the ECHR. In addition, they should be prescribed by law, necessary and proportionate to these legitimate aims. The protection of health is a legitimate aim that States may evoke to adopt measures restricting the right to freedom of assembly.

When a meeting or assembly has a religious nature, Article 9 of the ECHR also applies. This provision states that everyone has the freedom to manifest their religion or belief, either alone or in community, through worship, teaching, practice and observance. Any restrictions must pursue at least one of the legitimate aims under the second paragraph of Article 9. They must also have a legal basis in domestic law, and be necessary and proportionate to the legitimate aims at stake. The protection of health and the protection of the rights and freedoms of others are among the legitimate aims that public authorities may invoke.

Digital health passports may be used in ways that may conceivably both restrict and promote the exercise of these freedoms.

For instance, take the hypothetical scenario whereby public authorities require individuals to routinely display their health status (e.g. COVID-19 test results or vaccination records once these are available) to access public and private spaces. Based on their health status, some individuals may be allowed to move freely. By contrast, others may be barred from travel and prevented from accessing specific places within the territory of their country of residence, including churches and other areas of assembly.

Such restrictions on their freedom of movement, assembly and manifesting religion or belief can be motivated by public health interests, which constitute a legitimate aim under the ECHR. Still, such measures must have a clear legal basis in domestic law, respond to a pressing social need and be proportionate to the aim to protect public health.

Arguably, such measures should preserve the freedoms of those who do not have the disease, are immune to it (if supported by strong scientific evidence) or have been vaccinated (once a vaccine is available). Scholars have argued that restricting the freedoms of some individuals would be a valid ethical motivation as it would avoid restricting the freedoms of the whole population (Brown, Kelly, Wilkinson, & Savulescu, 2020).

However, would that be the least restrictive viable solution? Conceivably, requiring individuals to routinely display their health status may be less restrictive on their freedoms than imposing a

lockdown. However, to fully answer this question, it is crucial to examine the conditions linked to the implementation of digital health passports.

In this regard, the availability and affordability of COVID-19 tests and eventually, vaccines, are key aspects, as these directly inform the health status displayed by digital health passports. For instance, if some people cannot access or afford COVID-19 tests, they will not be able to prove their health status, thus having their freedoms de facto restricted.

Unless the tests and, once available, vaccines are accessible to all, any large-scale deployment of digital health passports risks disproportionately segmenting the society, and potentially breaching the rights to equality and non-discrimination, as discussed in the next section.

Equality and non-discrimination

Article 1 of the UDHR recognises that 'all human beings are born free and equal in dignity and rights.' International treaties on human rights such as the ECHR operationalise the right to equality by establishing guarantees against discrimination (Article 14 ECHR).

In the UK, the Equality Act 2010 provides a single legal framework for the protection of equality and the right to non-discrimination. It offers comprehensive protection against discrimination on the grounds of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation.

Digital health passports can have an important impact on the protection of equality and non-discrimination. Depending on how they are implemented, they may exclude a large segment of the population. Two key issues can be identified in this regard.

First, if individuals cannot access or afford COVID-19 tests and, once available, vaccines, they will not be able to use digital health passports. As discussed above, that could restrict their rights considerably if the relevant technology is used to determine, for example, who can or cannot travel, enter a workplace, and attend public or private gatherings such as sport events and church services.

Such outcomes would be compounded by the disproportionate effect that COVID-19 demonstrably has on Black Asian and Minority Ethnic (BAME) communities (Kirby, 2020; Pana, et al., 2020; Public Health England, 2020) and on the elderly (Armitage & Nellums, 2020; WHO, 2020b).

It is, therefore, crucial that the communities that have already been badly impacted by the pandemic have swift access to affordable tests and, eventually, vaccines. Otherwise, deploying digital health passports could further deepen the existing inequalities in society.

Second, digital health passports schemes relying on face recognition technologies to verify identity may also impact BAME individuals more severely.

For instance, research demonstrates that facial recognition technologies are still not accurate for recognition of Black and Asian faces and are significantly inaccurate when trying to recognise women with darker skin types (Buolamwini & Gebru, 2018). Such technical problems could have devastating consequences for individuals using digital health passports. They could also lead to unlawful discrimination on the ground of race, if there are no alternative ways to verify identity and if the providers insist on using inaccurate facial recognition technologies.

Accordingly, digital health passports should not rely solely on facial recognition technologies for identity verification, at least until these are not sufficiently accurate and legally compliant.

Policy Recommendations

The COVID-19 pandemic has exposed the need for policymakers to navigate a complex set of legal obligations while balancing competing rights and legitimate aims. This policy brief has examined the key issues arising from the protection of data privacy, the freedoms of movement, assembly and to manifest one's religion or beliefs, as well as the rights to equality and non-discrimination.

Analysis in this brief confirms that measures supporting the deployment of digital health passports interfere with these rights, but also that such interferences may be justified by public health interests if specific conditions are met. In this regard, policymakers must strike an adequate balance between protecting the rights and freedoms of all individuals and safeguarding public interests while managing the effects of the pandemic.

Accordingly, it is recommended that:

1. **Policymakers should require digital health passport providers to adopt appropriate technical and organisational measures and undertake data protection impact assessments to address potential data privacy-invasive situations proactively.**

   In doing so, they should take into account not only the potential risks for data privacy but also the situations in which the deployment of digital health passports is likely to result in a high risk to individuals' rights and freedoms.

2. **Policymakers should ensure the availability and affordability of COVID-19 tests and vaccines (once developed) to the whole population before any large-scale deployment of digital health passports.**

   Any failure to address the issues of availability and affordability of COVID-19 tests and vaccines risks dramatically excluding already vulnerable populations from protection and may disproportionately restrict the exercise of their legal rights.

References

Ada Lovelace Institute. (2020a). *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.* London: Ada Lovelace Institute.

Ada Lovelace Institute. (2020b). *International Monitor: Public Health Identity Systems.* Retrieved from Ada Lovelace Institute: https://www.adalovelaceinstitute.org/our-work/identities-liberties/international-public-health-identity-systems-monitor/

Armitage, R., & Nellums, L. B. (2020). COVID-19 and the consequences of isolating the elderly. *The Lancet Public Health, 256.*

Aschwanden, C. (2020). The false promise of herd immunity for COVID-19. *Nature, 587, 26-28.*

Beduschi, A. (2020). Immunity Passports: A Risky Solution. *Directions Cyber Digital Europe.* Retrieved from https://directionsblog.eu/immunity-passports-a-risky-solution/

Blackstone, W. (1775). *Commentaries of the Laws of England* (Vol. Volume 1). (D. Lemmings, Ed.) Oxford: Oxford University Press.

Brown, R. C., Kelly, D., Wilkinson, D., & Savulescu, J. (2020). The scientific and ethical feasibility of immunity passports. *Lancet Infect Dis, 1-6.* doi: https://doi.org/10.1016/S1473-3099(20)30766-0

Buolamwini, J., & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research Conference on Fairness, Accountability, and Transparency,* 81, pp. 77-91.

Busby, M. (2020, October 17). Digital 'health passport' trials under way to aid reopening of borders. *The Guardian.*

COVID-19 Credentials Initiative. (2020). *The COVID-19 Credentials Initiative.* Retrieved from https://www.covidcreds.com/.

Cownie, F., & Bradney, A. (2017). Socio-legal studies: a challenge to the doctrinal approach. In D. Watkins, & M. Burton, *Research Methods in Law* (pp. 40-65). London: Routledge.

Gruener, D. (2020). Immunity Certificates: If We Must Have Them, We Must Do It Right. *Harvard University Edmond J. Safra Center for Ethics. COVID-19 White Paper 8.*

Hannum, H. (1995). The status of the Universal Declaration of Human Rights in national and international law. *Georgia Journal of International and Comparative Law, 287-397.*

Iwasaki, A. (2020). What reinfections mean for COVID-19. *Lancet Infect Dis.* doi: https://doi.org/10.1016/S1473-3099(20)30783-0

Kirby, T. (2020). Evidence mounts on the disproportionate effect of COVID-19 on ethnic minorities. *The Lancet Respiratory,* 547-548.

Kofler, N., & Baylis, F. (2020). Ten reasons why immunity passports are a bad idea. *Nature, 581,* 379–381.

Magna Carta 1297 Chapter 9 25 Edw 1 cc 1 9 29.

McKay, D., Heisler, M., Mishor, R., Catton, H., & Kloiber, O. (2020). Attacks against health-care personnel must stop, especially as the world fights COVID-19. *The Lancet,* 1743-1745.

Moeckli, D. (2016). *Exclusion from Public Space. A Comparative Constitutional Analysis.* Cambridge: Cambridge University Press.

O'Connor, R. C., Wetherall, K., Cleare, S., McClelland, H., Melson, A. J., Niedzwied, C. L., . . . Robb, K. A. (2020). Mental health and well-being during the COVID-19 pandemic: longitudinal analyses of adults in the UK COVID-19 Mental Health & Wellbeing study. *British Journal of Psychiatry,* 1-17.

Pana, D., Sze, S., Minhas, J. S., Bangashd, M. N., Pareek, N., Divallg, P., . . . Pareek, M. (2020). The impact of ethnicity on clinical outcomes in COVID-19: A systematic review. *EClinicalMedicine,* 1-8.

Phelan, A. L. (2020). COVID-19 immunity passports and vaccination certificates: scientific, equitable, and legal challenges. *The Lancet,* 1595-1597.

Privacy International. (2020). *The looming disaster of immunity passports and digital identity.* London: Privacy International.

Public Health England. (2020). *Beyond the data: Understanding the impact of COVID-19 on BAME groups.* London: PHE Publications.

Stephens, D. S., & McElrath, M. J. (2020). COVID-19 and the Path to Immunity. *JAMA,* 1279-1281.

The National Archives. (2020) *Coronavirus Legislation.* Retrieved from https://www.legislation.gov.uk/coronavirus.

United Nations Network on Racial Discrimination and Protection of Minorities. (2020). *Leave No One Behind. Racial Discrimination and the Protection of Minorities in the COVID-19 Crisis.* Geneva: United Nations.

Venkataramakrishnan, S. (2020, May 24). Start-ups race to develop Covid-19 immunity passports. *Financial Times.*

WHO. (2020a). *Estonia and WHO to jointly develop digital vaccine certificate to strengthen COVAX.* Retrieved from World Health Organization: https://www.who.int/news-room/feature-stories/detail/estonia-and-who-to-jointly-develop-digital-vaccine-certificate-to-strengthen-covax

WHO. (2020b). *Preventing and managing COVID-19 across long-term care services.* Geneva: World Health Organization.

Disclaimer

This policy brief was produced by Dr Ana Beduschi, Associate Professor of Law at the University of Exeter Law School. It presents independent research funded by the Economic and Social Research Council (ESRC) as part of UK Research & Innovation's rapid response to COVID-19 (project title COVID-19: Human Rights Implications of Digital Certificates for Health Status Verification; project number ES/V004980/1).

The views and opinions expressed in this brief are those of the author and do not necessarily reflect those of the ESRC, the UKRI or the University of Exeter.

UNIVERSITY OF EXETER | LAW SCHOOL | RENNES DRIVE EX4 4RJ EXETER

Twitter: @ana_beduschi | socialsciences.exeter.ac.uk/law/research/projects/