HARVARD Kennedy School
CARR CENTER
for Human Rights Policy

JUNE 1, 2020 | ISSUE 05

Carr Center Covid-19 Discussion Series

Examining the Ethics of Immunity Certificates

Carr Center faculty and fellows examine the human rights implications and legal ramifications of introducing widespread immunity passports.

Mark Latonero

TECHNOLOGY AND HUMAN RIGHTS FELLOW, CARR CENTER

Elizabeth Renieris

TECHNOLOGY AND HUMAN RIGHTS FELLOW, CARR CENTER

Mathias Risse

FACULTY DIRECTOR, CARR CENTER

From a human rights standpoint, what are the benefits and downfalls of immunity passports? Which human rights are implicated by their introduction, and are any of their infringements acceptable, even temporarily?

LATONERO – An assessment of the merits of digital certificates to identify individuals with COVID-19 immunity must face the fact that any such system would be inherently discriminatory. Sorting out the population into those that have or don't have immunity would confer social advantages or disadvantages that would immediately implicate fundamental human rights. Classifying individuals based on immunity could determine who is free to travel, attend school, access a ballot box, go to court, or get back to work. One would be hard pressed to find that so-called immunity passports are a necessary or proportionate response to our current COVID-19 situation. Unless convincing evidence is presented, we should remain highly skeptical that immunity passports could be designed in such a way that leads to fair social outcomes

rather than unjust discrimination and stigmatization that exacerbates inequality. With so much at stake we must critically examine to what extent and under what conditions technology, and tech companies, should play a role. Building a national (or international) interoperable digital identity system that protects and upholds human rights and dignity would be an extremely difficult undertaking in the best of times, let alone in the middle of a global pandemic. We should see any proposal, pilot, or live beta release of digital immunity passports for what they are: experiments using unproven technologies on real people at scale during a real-time global crisis with clear risks to human rights and unknown consequences. As such, these technologies, their creators, and users, should be subjected to the highest levels of public scrutiny, accountability, and oversight. Practically speaking, any company or government developing digital immunity certificates must involve input from civil society and other experts who understand that the computational challenges for digital security, data protection, privacy, and identification cannot be separated from local political, legal, economic, and cultural contexts where these technologies will be deployed. Conducting human rights risk assessments, from the earliest design phases onwards, would provide both technologists and policymakers with local context, which is critical for decision making.

RENIERIS – The introduction of so-called "immunity passports" for COVID-19 would implicate an array of fundamental human rights. From the perspective of international human rights law, they could interfere with core civil and political rights, including the right to privacy and the freedoms of association, assembly, and movement, per the International Covenant on Civil and Political Rights (ICCPR). They would also implicate core economic, social, and cultural rights, such as the right to work, the right to an education, and the right to participate in cultural life, per the International Covenant on Economic, Social, and Cultural Rights (ICESCR). Immunity passports would also implicate related rights under various regional human rights frameworks, including the rights to liberty, privacy, and the protection of personal data, and the prohibition on discrimination, as provided by the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union, as well as the rights to equal protection and liberty, freedoms of association and movement, the right to work and education, and the freedom from discrimination under the African Charter on Human and Peoples' Rights. Even where not strictly mandatory, the introduction of immunity passports could seriously limit freedom and autonomy, as governments and other stakeholders come to rely on them to make decisions about what people can and cannot do. The threats to freedom and autonomy are further amplified where people have virtually no way of challenging determinations about their status that are foundational to the issuance of immunity passports. While fundamental, most of the human rights implicated by immunity passports are qualified and not absolute, meaning that derogations are permissible under limited circumstances, such as in times of war or a public emergency; the pandemic would clearly qualify as a public emergency. Nevertheless, derogations to permit interference with fundamental rights must satisfy three principles: they must be (1) prescribed by or in accordance with law (i.e. legality); (2) necessary to achieve a legitimate aim

There is presently no legal framework that could provide a sufficiently clear and precise standard to govern the use of such passports, or to ensure the protection of individual rights.

(i.e. necessity); and (3) proportionate to achieving that aim (i.e. proportionality); assessing proportionality includes whether less intrusive measures are available to achieve that aim. In contrast to the ICCPR, ICESCR, and various other regional human rights frameworks, the African Charter does not contain a derogation clause or provide for derogations, even in the case of public emergencies, complicating the application of these principles. Given the current state of public health and scientific research on SARS-CoV-2, COVID-19 disease, antibody testing, vaccine development, and what is known about immunity, there is insufficient evidence to support the necessity of immunity passports. Even where necessity could be established, immunity passports are rarely provided for other infectious diseases such as measles, making it difficult to satisfy the proportionality test. Moreover, there is presently no legal framework that could provide a sufficiently clear and precise standard to govern the use of such passports or to ensure the protection of individual rights, making it hard to satisfy the legality principle.

RISSE – I have become persuaded that the right way forward in resolving the coronavirus crisis is the testing, tracing, and supported isolation strategy advanced by the EJ Safra Center, among others. That is, people need to be tested at a large scale; we need to trace contacts of those who tested positive and test them as well; and everybody who does test positive needs to remain in isolation and receive the necessary support so they can manage during quarantine (including treatment if they become symptomatic). This comprehensive strategy for reopening the economy in a way that defeats the virus, if implemented the right way, is also responsive to human rights concerns. That is, testing would need to occur at a scale and manner that would not lead to concerns of discrimination, and restrict people—especially in their freedom of movement—only as long as needed on public-health grounds. Human rights standards also make clear what would be involved in supporting people throughout–and here human rights standards (rather than civil rights standards) indeed play especially important roles, because this kind of support would also need to accrue to undocumented people.

In light of all this, what kind of role could "immunity passports" play? They could certainly be useful for conveying that certain people no longer need to be tested, and thus also save valuable testing capacities. Still, for most scenarios, the availability of this information would not actually require any kind of passport, but rather ready access to relevant records. "Passports" are normally intended to generate a kind of access to places or services that otherwise would not be available. In scenarios where testing, tracing, and supported isolation are executed at a large scale, granting access to some people and restricting that of others would rarely, if ever, be necessary or proportionate. It would not be "necessary" in the sense that what it takes to keep people safe is not that those around them are immune, but that they are not currently infected. It would not be "proportionate" in the sense that the use of such passports would come with three distinctive disadvantages: (1) it would create incentives for people to get infected to obtain the benefits involved, including those

In scenarios where testing, tracing, and supported isolation are executed at a large scale, granting access to some people and restricting that of others would rarely, if ever, be necessary or proportionate.

who otherwise might have gotten by just fine until vaccination becomes available; (2) it would needlessly preclude people from accessing locations and services even though they are not infected, pose no health risk to others (and might even be immune but have not been tested yet); and (3), it introduces a new dimension of advantage in society that has a substantial potential of creating new kinds of social stigma (and resentment created in response to them)—which is best avoided unless absolutely necessary.

So in situations where testing, tracing, and supportive isolation are in place, there would be some limited use to such "passports," but their role should indeed be as limited as possible, and thus involve only conveyance of information rather than control of access. The spirit should be sufficiency rather than necessity. To avoid any larger relevance for passports, one should talk about "immunity certificates" rather than "passports." Their most prominent use (the point just made notwithstanding) might well be at border-crossings, as long as such crossings come with mandatory testing and such testing would be unnecessary for immune people. But that use should be in the spirit of sufficiency, not necessity.

What about scenarios where testing, tracing, and supported isolation are not implemented at a large scale? To begin with, one would hope the country in question will soon change its strategy. It is hard to imagine scenarios where immunity certificates can be issued at a large scale, but such testing itself cannot be done at such a scale. At the very least, countries that are in a position to issue immunity certificates but unable to test at a large scale should use previous and ongoing disadvantage among the most important criteria for being put in a position where such a certificate could be issued. In other words, in such a scenario, immunity passports should at least be partially used as a social policy tool. Otherwise the way in which a new dimension of advantage is introduced might prove rather pernicious going forward, channeling yet more advantage to the same people.

Are there legal frameworks that could provide sufficient protection against arbitrary use or misuse of immunity passports? What kinds of implementations, from a technical and governance perspective, would be necessary and proportionate to meet those ends?

LATONERO – It is likely the case that governments who are intent on using digital identity certificates for COVID-19 immunity will rely on private sector tech companies to build them. The existing legal frameworks are insufficient to address the array of human rights issues raised by immunity passports. Thus companies and their employees building digital immunity certificates may be confronted with situations where their technologies are used in ways that violate human rights. This may take the form of mission creep, where a technology designed to certify immunity status is repurposed by governments beyond the original intent, such as certifying immigration status. The UN Guiding Principles on Business and Human Rights provides a practical framework

for tech companies to uphold their responsibility to respect human rights. Regardless of whether a government client attests to the legality of a tech intervention, companies should conduct their own human rights due diligence. Using international human rights law and norms, companies should continually assess the potential and actual impact of their products on rights holders in each "market" or country. Risks should be assessed, identified, and mitigated. Mechanisms of redress and remedy should be established. Tech company lawyers can include sunset clauses in contracts. Engineers can include encode features that protect human rights, like privacy. And a company can also say no. Imagining a tech company refusing to provide services to a government with legal authority is not as far-fetched as it might sound. For example, Microsoft has said it turned down a contract to provide a law enforcement agency with facial recognition citing human rights concerns, Google has pledged not to pursue AI applications that contravene international human rights, and tech workers from a number of companies have refused to work on government projects that separate migrant children from parents. Human rights experts and advocates should be empowered to help identify the human rights risks of tech company interventions and provide a layer of accountability and oversight.

Human rights experts and advocates should be empowered to help identify the human rights risks of tech company interventions and provide a layer of accountability and oversight.

RENIERIS – Per the legality principle, measures that would interfere with fundamental human rights must be prescribed by, or in accordance with, law. While this does not always require the introduction of a new or bespoke law, existing laws must be sufficiently clear in scope and application to satisfy this principle. It is unclear that any existing legal frameworks could provide sufficient safeguards to govern the use and protect against the misuse of immunity passports at this time. Even the introduction of COVID-19 digital contact tracing apps, which implicate many of the same human rights as immunity passports would (albeit to a lesser degree), has demonstrated the insufficiency of most existing legal frameworks, including the perceived "gold standard" of data protection frameworks, Europe's General Data Protection Regulation (GDPR). For example, in the U.K. Parliament, the Joint Committee on Human Rights has opined that existing laws, including the U.K.'s Data Protection Act of 2018, which enshrines the GDPR into national law, provide an insufficient legal basis for the government's plans to roll out contact tracing apps given the unprecedented data gathering involved with such apps; bespoke legislation is required to provide robust legal protections for individuals about what data will be collected, how that data will be used, who will have access to it, and how it will be safeguarded from hacking and other security events. Likewise, in the United States, Congress is scrambling to draft bespoke legislation for COVID-19 contact tracing apps. In India, where plans for national data

Bespoke legislation would be necessary to address the broad set of risks posed by, and provide sufficient safeguards against the misuse of, immunity passports of any kind.

protection legislation have stalled, they would provide little protections against misuse of immunity passports anyway where such legislation largely exempts public sector or government uses of data, just as they would provide few protections against the government's invasive Aarogya Setu contact tracing app. Because immunity passports, like contact tracing apps, implicate a wide array of human rights beyond the rights to privacy and the protection of personal data, these existing frameworks provide insufficient safeguards against the risks of exclusion, discrimination, and stigmatization, among others. Bespoke legislation would be necessary to address the broad set of risks posed by, and provide sufficient safeguards against the misuse of, immunity passports of any kind.

RISSE – The age of Big Data has arrived, and it comes with endless opportunities. But we need to be vigilant that digital technologies use these data in ways that benefit people, including respect for human rights standards. One way of doing so is to make sure that people's personal data are always only used in the relevant context for which people explicitly authorized use, or could reasonably be presumed to do so. To some extent, making good on that will be a matter of governmental oversight—which then would have to be designed appropriately, including internal supervision. But the companies that design the relevant software should also do all they can to make transfer and mining of data across contexts very difficult.

The introduction of immunity passports would be one rather striking example of the kind of compulsory digitization that we are observing all around in response to COVID-19. Going forward, what should human rights activists be concerned about as this trend continues?

LATONERO – If by compulsory digitalization we mean subjecting people to digital systems in exchange for needed services without meaningful consent, what we are seeing in response to COVID-19 is an acceleration of a trend that has been going on for some time now. I found a number of examples in my research on digital identity systems for migrants and refugees. I observed how a family of asylum seekers arriving to the Greek Island of Lesvos from Libya were taken directly to the Moria refugee camp for identity processing where they were compelled by government officials to submit their biometrics in exchange for shelter and safety. Near the French-Italian border, I observed how migrants from East Africa actively avoided a camp run by an international aid organization because federal police were perched at the entrance collecting digital fingerprints from

Digital identity systems will have a disproportionate impact on marginalized and vulnerable people unless transparent and accountable safeguards are put into place from the very beginning and continually monitored.

anyone seeking food and medicine on the other side of the gates. My team and I interviewed legal aid organizations in Milan representing asylum seekers who were trapped in a bureaucratic nightmare—they could not access needed social services because their names were misspelled in a government database. In short, digital identity systems will have a disproportionate impact on marginalized and vulnerable people unless transparent and accountable safeguards are put into place from the very beginning and continually monitored. I find the arguments that digital identity systems are necessary to reduce fraud particularly worrying when it comes to COVID-19. Studies demonstrate that officials often operate under a tacit and pernicious assumption that marginalized groups, like the poor, are predisposed to fraud and therefore should be subjected to increased surveillance. I have written about the humanitarian crises in Yemen where international aid agencies claimed biometrics are necessary to prevent fraud perpetuated by displaced people in desperate need of food. Yet little evidence based research is offered as to the extent of the fraud and why a digital identity "solution" is necessary and proportionate. This has led to surveillance humanitarianism, which I describe as the development and deployment of massive data collection technologies during times of crises that inadvertently increase the risk, vulnerability, and insecurity of people in need. Human rights researchers and civil society are essential to bring to light the risks and harms of COVID-19 technologies on the most vulnerable, which serve as a harbinger for what's in store for the broader segments of the population should immunity passports become required by national governments.

RENIERIS – Compulsory digitization is an alarming trend that poses clearly heightened risks of exclusion, discrimination, and stigmatization to people around the world; those on the wrong side of the growing digital divide end up effectively shut out of society and the benefits of digitization. But there is another, underappreciated risk. Unlike cash or non-digital objects, which are static and capable of being fully owned and controlled by their possessor, digital cash and digital objects rely on software and a host of intermediaries who mediate their use. In this way, compulsory digitization also poses serious risks to privacy, liberty, and autonomy, as digital systems are never fully in the control of the individuals who are forced to rely on them. Rather, these tools are always subject to external interference, surveillance, and manipulation. If we are going to mandate digitization, human rights activists must demand that these tools are built with the interests of people in mind. This means embedding core human rights principles into the design and development of digital technologies. It also means abandoning the myth of technology neutrality, acknowledging the unprecedented power of these tools to shape our decisions and actions, and recognizing that all design choices have consequences, either nudging us to act in alignment with our own interests or sludging us to act against them. As a result, we will also need new legal interventions and guardrails, including an upgraded view of applying human rights to the digital reality.

Those on the wrong side of the growing digital divide end up effectively shut out of society and the benefits of digitization.

RISSE – Yes, of course. We must always be vigilant that new technologies are used in ways that benefit people, and we must spell this out in ways that involve human rights protections. To repeat a point I just made, one crucial task here is to make sure that people's personal data are always only used in the relevant context for which people explicitly authorized use, or could reasonably be presumed to do so. To some extent, making good on that will be a matter of governmental oversight (which then would have to be designed appropriately, including internal supervision). But the companies that design the relevant software should also do all they can to make transfer and minability of data across contexts very difficult.