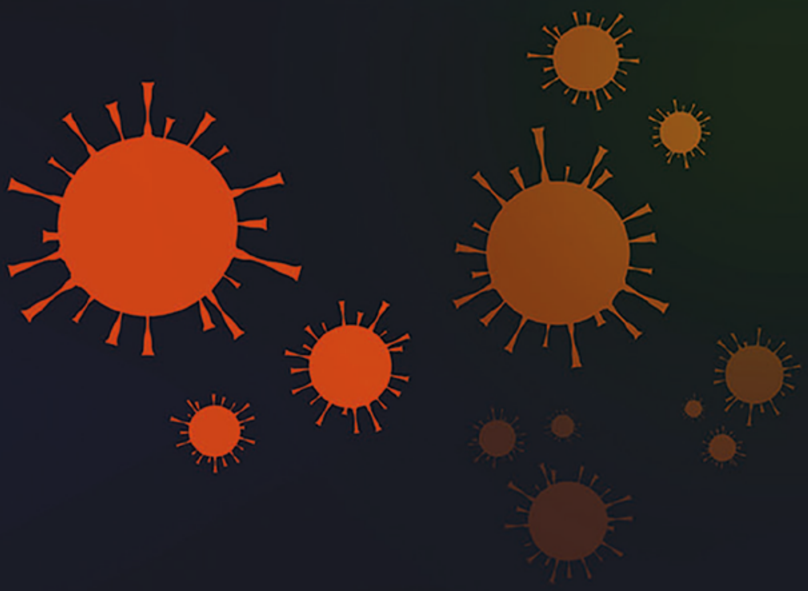
SSRC



Surveillance and the ‘New Normal’ of Covid-19: Public Health, Data, and Justice

Surveillance and the ‘New Normal’ of Covid-19: Public Health, Data, and Justice

SOCIAL SCIENCE RESEARCH COUNCIL

This publication is available online at **ssrc.org/PHSHR-report**.

Please direct inquiries to:

Social Science Research Council
300 Cadman Plaza West, 15th Floor
Brooklyn, NY 11201
Telephone: 212-377-2700

Email: info@ssrc.org
Web: www.ssrc.org

The world marks one year of the Covid-19 pandemic with both hope and apprehension. New coronavirus variants threaten to undo the halting progress of the past year, while new vaccines raise the prospect of an end to the crisis. Yet even when the pandemic does subside, we must reckon with the fact that the society that emerges will be profoundly different than the one that came before it. In myriad ways, daily life as we know it will have been fundamentally, and permanently, transformed.

In an effort to document, contextualize, and understand the impacts of the pandemic as they unfolded, in April 2020, the Social Science Research Council launched the **Virtual Research Center on Covid-19**. This multifaceted initiative is an effort to bring this knowledge of the social sciences to bear on the various changes that have been prompted or hastened by the pandemic.

Among these transformations was a rapid expansion of the use of surveillance technology in public health. Many of these efforts, while critical to slowing the virus's spread, also raised difficult questions about how to balance privacy with transparency, the individual with the collective, and urgency with deliberation. To address these issues, in June 2020, the Council convened the **Public Health, Surveillance, and Human Rights Network**, an international group of forty leaders in industry, civil society, government, and academia who shared their diverse experiences and expertise in a series of discussions over the course of two months.

The virus's rapid spread necessitated equally swift responses in the form of closures, mask mandates, and large-scale data collection. As the world hurtled toward a markedly new normal, the network meetings provided an opportunity to pause and consider the implications of the changes we were witnessing for privacy, human rights, and justice worldwide. *Surveillance and the 'New Normal' of Covid-19* is a distillation of these cross-sector, transnational conversations.

This report, and the deliberations that inform it, would not have been possible without the support of an array of stakeholders. I am deeply grateful, first and foremost, to the members of the PHSHR Network for this work. Many thanks as well to the members of the Council's SSRC staff, especially David A. Banks, Alexa Dietrich, Rebecca Tave Gluskin, Clara Hanson, Ronald Kassimir, Renee King, Duncan Omanga, Michael Miller, and Vina Tran. The network was made possible by a partnership with the John D. and Catherine T. MacArthur Foundation, the Ford Foundation, and the Henry Luce Foundation.

Scientists and technologists have rapidly developed critical tools that promise to end this pandemic. But implementing these tools effectively and equitably requires a deep understanding of the complex social, economic, and political processes undergirding diverse societies across the globe. While countries and communities have taken diverse tacks to addressing the pandemic, this moment is a stark reminder of our interconnectedness.

Only by pooling our collective knowledge—across disciplines, across sectors, and across nations—will we overcome this crisis while advancing the common good and emerging stronger as a result. This report signals a first step towards those efforts.

Alondra Nelson

Alondra Nelson
President
January 2021

I. INTRODUCTION

The Covid-19 pandemic has dramatically altered the way nations around the world use technology in public health. As the virus spread globally, some nations responded by closing businesses, shuttering schools, limiting gatherings, and banning travel. Many also deployed varied technological tools and systems to track virus exposure, monitor outbreaks, and aggregate hospital data.

Some regions are still grappling with crisis-level conditions, and others are struggling to navigate the complexities of vaccine rollouts. Amid the upheavals, communities are adjusting to a new normal, in which mask-wearing has become as commonplace as seatbelt use and digital temperature checks are a routine part of entering public buildings.

Even as the frenzy of emergency responses begins to subside, the emergent forms of surveillance that have accompanied this new normal persist. As a consequence, societies face new questions about how to manage the monitoring systems created in response to the virus, what processes are required in order to immunize populations, and what new norms the systems have generated. How they answer these questions will have long-term impacts on civil liberties, governance, and the role of technology in society. The systems implemented amid the public health emergency could jeopardize individual freedoms and exacerbate harms to already vulnerable groups, particularly if they are adapted to operate as permanent social management tools. At the same time, growing public awareness about the impact of public health technologies could also provide a catalyst for strengthening democratic engagement and demonstrating the urgency of improving governance systems. As the world transitions in and out of pandemic crisis modes, there is an opportunity to think broadly about strengthening public health systems, policymaking, and the underlying structure of our social compacts.

The stakes are high: an enduring lesson from history is that moments of crisis often recast the roles of governments and the rights of individuals. In this moment of flux, the Social Science Research Council calls on policymakers, technologists, data scientists, health experts, academics, activists, and communities around the world to assess the implications of this transformation and seize opportunities for positive social change. The Council seeks to facilitate a shift from reactive modes of crisis response to more strategic forms of deliberation among varied stakeholders. As such, it has convened discussions and directed research in order to better understand the intersection of governance and technologically enabled surveillance in conditions of public health emergencies. Through these activities, the Council aims to provide analysis that can help foster societies that are more resilient, democratic, and inclusive and can, therefore, better withstand future crises.

"Moments of crisis often recast the roles of governments and the rights of individuals."

With these goals in mind, the Council convened a cross-disciplinary, multinational group of experts in the summer of 2020 to survey the landscape of human rights and social justice with regard to technologically driven public health practices. The resulting group—the **Public Health, Surveillance, and Human Rights (PHSHR) Network**—raised a broad range of questions about governance, social inequalities, data protection, medical systems, and community norms: What rules should govern the sharing of personal health data? How should the efficacy of public health interventions be weighed against the emergence and expansion of new forms of surveillance? How much control should multinational corporations have in designing and implementing nations' public health technology systems? These are among the questions that pushed members to think beyond traditional professional, geographic, and intellectual boundaries.

The PHSHR Network developed a mode of discussion that paired big-picture, comparative thinking with concrete analyses of specific contexts and issues. A wide range of technological responses have emerged to combat the pandemic, from health-check apps and wearable devices to thermal cameras and facial-recognition temperature checks to screen for access to public places. Many of the core challenges of the pandemic's 'new normal' have come to the fore in debates about contact tracing, a public health intervention that shows the trade-offs between community interests and individual rights. While contact tracing has been around for centuries, new forms of digital tracing use tools such as Bluetooth and geolocation data to track an infected individual's proximity to others (see: **Manual Contact Tracing** and **Digital Contact Tracing**).

The new tracing technology carries upsides: it may provide powerful tools for informing individuals at risk of infection, and it can alert exposed individuals more systematically—and, in some instances, with more privacy—than manual contact tracing. At the same time, digital contact tracing carries downsides and risks: it tends to focus interventions on owners of smartphones, at the risk of neglecting already vulnerable populations who lack access to such technologies. It necessitates secure systems for storing and analyzing sensitive health data. And it requires public trust in technology, corporations, and political systems.

Many of the contact-tracing programs that emerged in response to Covid-19 were created without clear evidence demonstrating their effectiveness or even explicit standards by which to evaluate their efficacy. The programs have also raised questions about the consequences of measurement errors, their effectiveness compared to manual contact tracing, and the utility of "exposure notification" in the absence of more thorough social support services.

MANUAL CONTACT TRACING

Contact tracing is a long-standing public health process that involves the collection and use of personal information to identify people who may have been exposed to an infectious disease. The information collected may involve sensitive data, such as health status, personal contacts, and daily whereabouts. As a result, contact tracing inevitably raises questions about privacy—questions such as:

- What information is collected and by whom?
- How long is the information retained?
- Who has access to the information?
- How is the information used?
- How much agency do individuals have within contact-tracing systems?

Manual contact tracing has been used since at least the mid-nineteenth century in Europe and for nearly a century in the United States to locate and notify individuals who have interacted with someone who has tested positive for an infectious disease. Traditionally, locating and monitoring functions were performed in person, which gave rise to the moniker "shoe-leather epidemiology." Manual contact tracing involves identifying and interviewing a person who is carrying a virus to identify those with whom that person had recently been in contact, informing those contacts, and repeating the process.

Manual intervention has been effective at controlling the spread of Ebola, SARS, HIV, and other infectious diseases, but the approach has limitations. It is time consuming and labor intensive, and its effectiveness depends on human memory to reconstruct contacts and potential exposures.[I] While the methodology can give people more control over sharing their information than digital contact tracing, individuals can also undercut the effectiveness of public health measures. In New York City, for example, it is estimated that only two out of every five people with the virus shared information with contact tracers.[II]

Further, manual contact tracing does not preclude privacy risks. Information collected can be disclosed to other people and institutions, causing material harm and undermining trust.[III] Information collection may be more comprehensive than necessary, and intensive collection can create greater risk of loss of anonymity or data reuse.[IV] Relying on institutions to collect information and alert potentially infected contacts also creates power imbalances between individuals and institutions that, at times, can be as strong as mandating participation in contact-tracing efforts.[V]

“Designing effective social interventions requires constant recalibration, conscientious governance, and a commitment to justice.”

Digital contact tracing provides one obvious entry point for the discussion of the stakes of technologically enabled public health surveillance. However, the questions raised by these tools are not just about specialized apps designed for this particular crisis. They are linked to larger social issues about the role of technology in improving population health and supporting rights and liberties more generally. Surveying the existing landscape of the varied global responses to the pandemic, including programs like contact tracing, allows us to better identify the implications and contexts of particular policy choices and to create a foundation for more informed responses in the future.

The Council has established several goals in this analysis of pandemic responses:

- **Improve health justice** by advancing principles for access to public health resources in a manner free from unbridled surveillance
- **Identify strategies** for responsible use of technology in public health crises
- **Frame issues** for future inquiry and research about the balance of privacy and rights with public health efficacy

In advancing these goals amid the pandemic, this report is both grounded in the present moment and forward-looking. This report does not seek to offer a comprehensive guide to particular technologies or policy responses. Instead, it maps a range of social fault lines and data-related challenges that the pandemic has raised. In the process, it highlights some emerging best practices and lessons learned that can guide future emergency responses. These include:

- Renewal of social compacts
- Consultation and collaboration
- Transparency
- Data minimalism
- Efficacy criteria and assessments

None of these strategies represent silver-bullet solutions to emergencies. Instead, the principles that emerged from the work of the PHSHR Network underscore that designing effective social interventions requires constant recalibration, conscientious governance, and a commitment to justice.

DIGITAL CONTACT TRACING

Digital contact-tracing programs bring into sharp relief some of the tensions between protecting individual privacy and safeguarding the right to health. The technologies—defined as efforts that rely significantly on digital tools to collect data and notify contacts regarding exposure to infected persons—have created new methods for conducting contact tracing, which carry the potential to improve health outcomes. Technology can automate all or part of contact-tracing efforts. For example, automated contact tracing uses technologies like smartphones or wearables to passively record where someone has been or with whom they have been in contact. It uses that information to identify potential contacts if the person becomes infected with the novel coronavirus. Proponents of automated approaches argue they have the potential to scale to large populations quickly, identify at-risk individuals rapidly, and are more accurate than human memory.

In some societies, participation in contact-tracing systems is mandatory, not voluntary. In Thailand and Malaysia, for example, participation in digital-hybrid contact tracing was a requirement to end lockdowns. In Singapore, participating in digital-hybrid contact tracing is required to enter places like supermarkets, schools, and offices.[VI] There are also a wide range of subnational uses of digital contact tracing.

II. PROCESS

Beginning in June 2020, the Council convened a network of 40 experts to identify emerging issues related to public health, surveillance, and privacy in response to the Covid-19 pandemic. Members came from diverse geographic contexts and fields, and they included people working on the front lines of various aspects of pandemic responses—South Korean and Australian legal scholars, Silicon Valley technologists, US and UK health experts, Thai and US data justice advocates, and Swedish and UK social researchers, to name just a few.[1] The group met weekly for two months to share perspectives on critical global challenges and opportunities that have arisen due to the pandemic.

The Council facilitated the PHSHR Network by providing a series of research briefings on surveillance issues related to the pandemic. These primers—which ranged from historical and comparative reviews of privacy norms and contact-tracing approaches in North America, Asia, Australia, and Europe to a survey of pandemic responses across the continent of Africa—informed the Network's deliberation (see **Appendix**).

The effort was made possible by a partnership with the John D. and Catherine T. MacArthur Foundation, the Ford Foundation, and the Henry Luce Foundation. Together with these partners, the Council has committed to mapping the risks, challenges, and opportunities posed by the public health surveillance crucial to stemming the pandemic. This report represents an initial step in disseminating the Network's discussions, raising awareness, sparking debate, engaging policymakers, and encouraging research about the changing role of technology in a post-pandemic society.

III. CONTEXT: THE POLITICS OF SURVEILLANCE

Governments around the world have experimented with restrictions on civil liberties, ranging from mild to draconian, with the stated aim of protecting the health of their communities during the pandemic. The result has been a bevy of "experiments" and the development of techniques that will remain in governments' arsenals, according to political scientist Adam Przeworski. In the future, governments "may or may not use what they will have learned, but they will have learned."[2]

A resounding lesson from history is that governments do not easily relinquish powers they acquire during emergencies. Therefore, such emergencies represent critical junctures to assess lessons learned, adapt policy, and challenge troubling trends. Further, technologies marshaled in response to the global pandemic threaten to accelerate the concerning normalization of surveillance and technological encroachments on civil liberties around the world. Already, some governments have allowed information gathered for public health purposes to be accessed by law enforcement or intelligence services.[3]

Amid the Covid-19 crisis, governments have placed extraordinary limits on liberties and rights. Some of the most obvious have involved restrictions of mobility—stay-at-home and lockdown measures, border closures, curfews, and bans on international travelers, for example. In a few nations, including the United States, masking mandates have spurred controversy and resistance in the name of freedom.

Technologically enabled public health measures augmented these restrictions and have included a variety of approaches to require information disclosures from citizens. For example, in South Korea, the government can criminally prosecute and fine people suspected of having Covid-19 who refuse to take diagnostic tests. Singapore's contact-tracing program, TraceTogether, links phone numbers with interaction data based on Bluetooth signals, and is required to enter some workplaces, schools, healthcare facilities, and other public spaces.[4]

These apps generate data that is valuable for public health but may also be commodified and used in an unintended fashion. Major data-gathering initiatives typically require partnerships between governments and private companies to create new digital infrastructure, develop software, and manage data collection. In many jurisdictions, government-corporate partnerships unfold with little accountability or transparency, raising questions about who ultimately owns the data and how it will eventually be used. The dramatic expansion of data gathering in response to Covid-19 has intensified many concerns about the threat of surveillance to individual freedoms.

“Amid the Covid-19 crisis, governments have placed extraordinary limits on liberties and rights.”

The advancement of public health has always required balancing between community oversight and the exercise of rights and liberties. However, how to best negotiate the tradeoffs between protecting the public and safeguarding individual freedoms is rarely clear and depends on the culture, laws, and privacy contexts of a particular community. How do local laws define individual and community privacy? How much value do institutions and community traditions place on that right? What past experiences have framed a society’s approach to privacy and public health?

A broad international consensus affirms the existence of a right to privacy, but national legal traditions vary markedly in their interpretations of privacy (see: **Global Privacy Norms**). These different norms have a profound effect on how governments model public health systems and what kinds of extraordinary measures are deemed appropriate during a crisis.

Pandemic Precedents for the ‘New Normal’

On-the-ground examples of how different nations have navigated public health surveillance and data management amid the pandemic are instructive. Nations learn from prior public health crises. While these experiences may make them more prepared for future pandemics, they may also usher in permanent transformations to rights and liberties. Ebola, HIV, malaria, and MERS represent just a few recent crises that have influenced nations’ responses to Covid-19.

South Korea provides a prime example. After the country became ground zero of MERS in 2015, the government drew criticism for its ineffective response to the outbreak. Subsequently, it developed a more strategic response, the Infectious Disease Control and Prevention Act (IDCPA). The 2015 law, which was later amended to address Covid-19, lays out a number of public rights and government responsibilities. It establishes that the public has the right to know about the spread of infectious diseases and a right to receive diagnoses and treatments at the government’s expense. The law also grants the government additional powers and conveys new obligations, such as the ability to shut down risky events or venues and the duty to disinfect dangerous sites.[5] The statute established amid the MERS outbreak allows the government to collect vast amounts of personal data without subjects’ consent or judicial warrant. CCTV footage, cell phone records, geolocation information, and credit card receipts are among the data sources authorized.[6]

The legal framework created amid MERS impacted South Korea’s Covid-19 response. As of January 2021, the nation has seen less than 1,500 Covid-related deaths in a country of over 51 million, and it has avoided some of the severe lockdown measures that many countries

GLOBAL PRIVACY NORMS

The United Nations established an explicit “right to privacy” in the Declaration of Human Rights in 1948, which was codified in the International Covenant on Civil and Political Rights in 1966. As new digital technologies created a host of privacy-related challenges, the UN General Assembly passed a resolution in 2013 to establish “the right to privacy in the digital age.”[VII] As of January 2021, 145 countries have data privacy laws meeting minimum international standards. But a sampling of different national traditions reveals that a one-size-fits-all approach to digital privacy and public health technology cannot accommodate the range of global understandings of privacy rights.

The United Kingdom and the European Union have adopted a general legal framework for data privacy that can be adapted to different sectors, such as medicine or financial services. The 2016 General Data Protection Regulation (GDPR) is the prevailing standard within the European Union and has influenced the privacy standards of many nations around the world. The GDPR uses a risk-based, context-specific approach. As a general rule, it does not allow collection of individuals’ health data without explicit consent, except under specific conditions related to safeguarding the public interest.

Legal traditions in the United States tend to regulate privacy sector by sector and hold health data as the most comprehensively regulated. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is the primary piece of national legislation that regulates health data in the US. HIPAA creates standards for proper storage, use, and transmission of personal health information.[VIII] For example, HIPAA restricts healthcare providers’ sharing of information to the extent minimally necessary for treatment, payment, or healthcare operations.[IX]

Around the world, nations have adopted a wide range of approaches to safeguarding privacy. The GDPR has influenced new data privacy regulations in a number of countries, such as India and Japan.[X] But considerable variance exists. For example, cybersecurity laws in China involve the principle of sovereignty, such that some types of “critical” infrastructure involved in gathering or creating personal information must be stored in China.[XI] These differences help explain why some nations have mandated the downloading of contact-tracing programs, while others rely on voluntary models.

adopted.[7] Some people credit the nation's effective pandemic response to the implementation of surveillance provisions and its vigorous early testing efforts.[8]

South Korea's approach to surveillance and enforcement is not without criticism. The country's National Human Rights Commission condemned the publication of detailed personal data—but not necessarily the collection of it.[9] And some international observers have also raised concerns about the privacy risks.[10] Nonetheless, polls of South Korean citizens suggest the public largely supports the government's approach.[11]

The Ebola and HIV crises in different parts of Africa have also shaped nations' responses to Covid-19. For example, several African nations have adopted a militarized approach to combating the virus and imposed harsh lockdowns—some of which led to more initial deaths from police violence than from the virus itself.[12] West African countries like Liberia, Sierra Leone, and Guinea activated tracking, tracing, and isolation methods honed during the 2014 Ebola outbreak.[13]

Even though the United States lacks extensive recent experience with a pandemic, several health-related emergencies spurred the creation of legal precedents that have affected US Covid-19 responses. The nation's legal foundations for crisis-related data sharing emerged after the September 11, 2001 attacks and Hurricane Katrina. Both events necessitated new forms of information exchange among medical providers that raised concerns about potential violations of individual privacy. In addition, concerns about bioterrorism after September 11 prompted the government to build a new infrastructure for sharing medical data between hospitals and public health agencies. The National Syndromic Surveillance Program (NSSP) was designed to consolidate the collection of health information into a nationwide, cross-sector system.[14] Funding for the NSSP languished, however, and by the time Covid-19 emerged, only 70 percent of US hospitals were providing data to the national system.[15] Underfunding and low usage of the system contributed to the nation's decentralized response.[16]

As these historical examples reveal, emergency responses have reframed rights and patterns of governance, often in ways unanticipated by their creators and unforeseen in their original contexts. Given the importance of historical precedents in shaping future responses, this report reflects on Covid-19 responses and considers the way that associated policies have impacted governance, social justice, and the protection of individuals.

IV. INEQUALITIES IN HEALTH

Vulnerable populations have been hit hardest by the global pandemic. One study estimated that in the United States, residents of poorer, substantially non-white counties are nearly eight times more likely to be infected with Covid-19 than residents of poorer, substantially white counties.[17] Likewise, in the United Kingdom, the Covid-19 mortality rate among Black African or Black Caribbean people was two and a half times higher than the rate for white individuals in the first part of 2020.[18]

Pandemic-related inequality extends much further than just the likelihood of becoming infected. In parts of the world already grappling with food insecurity, the economic downturn unleashed by the pandemic has brought new levels of malnutrition and hunger. The United Nations World Food Program expects the number of people experiencing life-threatening food insecurity in the developing world to nearly double in a single year amid the pandemic.[19] Pandemic responses threaten to do further harm to already disenfranchised groups if greater consideration is not given to the burdens imposed by physical isolation, the digital divide, surveillance exposure, and humanitarian risks.

For many, physical isolation—one of the most common ways to minimize Covid-19 exposure—is not possible. Essential workers such as healthcare providers and public transit employees must share space with other people to provide important services. Quarantining may place disproportionate burdens on those who cannot work from home or who do not have the financial or social resources to remain isolated. As those who cannot physically isolate may disproportionately live in under-resourced neighborhoods and in more crowded conditions, the effect of prior vulnerabilities is exacerbated.[20]

Throughout the health crisis, digital divides have magnified social inequalities on both global and local scales. Smartphones have become vital technologies for accessing social resources and gaining visibility to policymakers.[21] Yet more than half the world's population lacks smartphone access. Further, within rich nations, the unequal patterns of smartphone access result in neglecting or underserving demographics such as the poor and elderly.[22] In Singapore, a TraceTogether wearable device was devised to create a notification system for populations less likely to have smartphones; however, the technology carries the risks of continuous surveillance.[23] Thus, the potential gains of digital contact tracing, such as exposure notification, tend to be distributed unequally and create additional challenges for those who already lack access to social resources.

Marginalized groups are subject to more surveillance beyond public health systems. In the United States, poorer individuals must share information in order to access public resources, such as food aid, public housing, or Covid-19 testing, and police disproportionately surveil Black and brown communities. Already surveilled groups may be unable to opt out of medical tracking and other surveillance systems. In Singapore, for example, migrant workers were required to download the nation's contact tracing application, TraceTogether, in order to go to work. The government has made it a crime for those who test positive for Covid-19 to refuse to assist the Ministry of Health in mapping their movement. The regulations require migrant workers to use the app, and this mandate comes in the context of enduring racism and xenophobia toward Indian and Bangladeshi workers.[24] Responses to the pandemic have intensified the data burden on groups that were already at risk of intrusive monitoring.

"Pandemic responses threaten to do further harm to already disenfranchised groups."

Also troubling are the risks of "humanitarian surveillance."[25] African nations have long served as sites of experimentation among aid agencies, academic researchers, technology developers, and others seeking to improve crisis responses. Although there have been many humanitarian technology success stories, successes are accompanied by failures in mission creep, privacy, and data security. Prior to Covid-19, experiments around disease surveillance using mobile phone data were used to tackle malaria in Zanzibar and Namibia, for example.[26] The interventions raised complex questions about data security and privacy that have returned during the present pandemic.[27] Calls from humanitarian organizations, academics, and journalists to aggregate sensitive mobile phone call detail records during the Ebola epidemic in West Africa overstated the value of the technological intervention and elided the rights and legal consequences of data sharing.[28] Further, the involvement of corporations and for-profit entities in such tracking efforts risks further privatizing public health systems and commodifying healthcare. Under this transformation of the social compact, members of under-resourced communities are compelled to submit to constant surveillance in exchange for access to medical services.

Vulnerable groups may have legitimate reasons to evade surveillance and distrust government institutions. Many have experienced disproportionate punishments outside the legal system and, as a result, seek to avoid encounters with government agencies and law enforcement. Fears of deportation or job loss can also create distrust and undercut the effectiveness of public health responses. Contact tracers in Los Angeles found that, owing to fear, in a typical week, nearly one-third of Covid-positive individuals did not respond to phone calls, and more than half refused to provide names of contacts.[29]

Improving pandemic responses will require accounting for the varied impacts of the virus on vulnerable populations and a better understanding of the ways in which health interventions have exacerbated existing inequalities and privacy concerns.

V. CHALLENGES IN GOVERNANCE

Governments around the world have been confronted with the difficult task of meeting the public health emergency posed by Covid-19 while also protecting civil liberties, preventing injustice, bolstering economies, and sustaining the institutions necessary for democratic societies.[30] Liberties are never absolute, and the policies instituted to address the current crisis frequently restrict rights to privacy, freedom of movement, and freedom of assembly—which may in turn restrict religious practice, political organizing, and the ability to avoid profiling and discrimination.[31]

Conversely, government inaction—protecting individual liberties rather than implementing pandemic responses—can infringe on the human right to health.[32] In the scramble to navigate a path between the two extremes of imperiling public health and suppressing liberties, many governments struggled to find an appropriate balance.

A common challenge has involved how best to implement contact-tracing programs and other public health ordinances quickly and at large scales. Mandatory compliance with policies such as mask-wearing and mobility restrictions have been common, and many governments have taken the additional step of criminalizing noncompliance. Many countries have used fines to enforce a variety of public health measures, such as quarantine orders and contact-tracing cooperation. Israel, for example, issued fines equivalent to USD$140 for failure to comply with lockdown measures.[33] Australia has issued fines for USD$1,150 for breaching lockdown orders.[34] In March 2020, the Polish government required quarantined individuals to upload selfies to an app to demonstrate compliance with lockdown orders or face fines up to USD$1,100.[35] South Korea may issue fines of up to USD$8,100, jail time for citizens, or deportation for non-citizens for violating self-quarantine rules.[36] Imprisonment is an especially troubling enforcement mechanism, as incarcerated populations are among the most vulnerable to contracting Covid-19.[37]

Compliance can be instituted not just in terms of legal mandates, but also in measures that predicate the delivery of social services on compliance with data collection. In India, for example, installation and use of the Aarogya Setu app is putatively voluntary. Yet the app is necessary for daily life. Government workers and many employees of private companies could face job loss for refusing to use it. Privacy experts also worry about businesses' reliance on contact-tracing applications and third-party facial recognition thermometers as a condition for entering spaces such as supermarkets, malls, schools, and doctor's offices.

The rise of criminalization and militarization of some nations' pandemic responses have heightened concerns about eroding civil liberties. Political leaders often frame discourse about the pandemic in terms of military or national security, and the framing invites the involvement of police and military actors. In the Philippines, police conducted house-to-house searches to identify people with Covid-19 and bring them to isolation facilities, under threat of imprisonment for failing to cooperate.[38] The president also used pandemic-related emergency powers in order to pass an anti-terrorism bill that allows suspects to be detained without a judge's approval for up to two weeks.[39] Military responses are also troubling to the extent that they prioritize an inward-looking security focus at the expense of international cooperation.

Public health surveillance technologies are also susceptible to exploitation for political gain. Some authoritarian regimes, for example, have used health technology sourced through intermediaries to surveil, target, harass, and, in some cases, imprison journalists and members of opposition groups. Zimbabwe passed a statute that enabled imprisonment of people circulating pandemic-related "information deemed false by the government," and the law has been used to sanction journalists and political opponents.[40] Pandemic responses in China, Guinea, and Ethiopia have included limitations on public access to information through bans of social media and other technologies and websites.[41]

The pandemic has also motivated greater use of controversial facial recognition technologies in China, Russia, Zimbabwe, and the United States, among other places. Widespread use of these technologies could normalize programs that are "deeply intrusive" and enable "widespread and bulk monitoring, collection, storage and analysis of sensitive personal data without individualized reasonable suspicion," according to Natalia Zviagina, director of Amnesty International's Moscow Office.[42]

The problem lies not only with authoritarian governments; democratic regimes around the world have exploited pandemic-related information collection and other powers for political gain. In the United States, for example, pandemic responses were often shaped to meet partisan ends, such as suspending abortions by categorizing them as nonessential medical procedures, loosening environmental regulations, and using quarantine in border control.[43]

Governments may also use the pandemic as a pretext to collect data that could be misused in the future. In New York, when Covid-19 testing capacity could not meet the high demand of residents, people could be prioritized for testing if they admitted to attending a protest. Civil rights advocates also claimed that law enforcement used pandemic measures as a pretext to limit protests.[44] The measures have troubling implications in the context of growing government surveillance of demonstrations by the Movement for Black Lives in response to the police killings of George Floyd and Breonna Taylor, among many others.

Addressing a contagious and deadly pandemic is paramount, but governments can abuse the powers granted to them for political advantage by suppressing the rights and liberties of residents. Companies and other nongovernmental actors may similarly use pandemic response as a pretext for commercial gain unless societies are mindful about what information is collected, by whom, and for what purposes—and when this data should be relinquished or deleted.

VI. DATA PROTECTION

In order to design effective pandemic responses, policymakers need information quickly and at large scales. However, widespread, coordinated data collection can also subject individuals to many forms of discrimination and mistreatment if that information is misused. While strong security measures are essential for protecting individual rights and privacy, responsible data collection involves much more than just security from data breaches.

The challenges are multinational and multisectoral. Successful data protection aligns the interests of states, private corporations, and individuals for the benefit of all; however, when the equilibrium is disrupted, individuals' privacy—and particularly data protections for vulnerable groups—tends to suffer.

For example, state actors and private companies can pool their resources to create vast processing systems to serve public health interests. The pandemic has already given rise to partnerships between governments and multinational corporations that raise questions about transparency and accountability. For example, Huawei has provided artificial intelligence–backed surveillance technologies to Botswana, Ghana, Uganda, Rwanda, Ivory Coast, Mauritius, Nigeria, South Africa, Algeria, Kenya, Morocco, Zambia, and Zimbabwe.[45] And widespread use of programs from Apple and Google in the Global South has prompted backlash against a new "data colonialism" from the Global North.[46]

Private corporations can also work at cross-purposes from state interests, to the detriment of the public good. Given their resources and capabilities in technology development, businesses have played an essential role in building data-collection tools needed to launch pandemic responses. However, health information collected in these efforts can easily be misused for profiteering when combined with targeted advertising programs, price-discrimination algorithms, or insurance assessments that may result in denials of coverage. The state of North Dakota offered a prime example with its Care19 contact-tracing app. Although users were told their privacy was secured, the app actively shared location and unique identifier data, as well as smartphone users' personal information, with at least three technology companies, including Google and Foursquare.[47]

In order to avoid the risks of ceding control to a foreign multinational corporation, France developed a proprietary app; however, the app cannot implement its full functionality due to the restrictions Apple places on access to iPhone Bluetooth data. “Why are Google and Apple dictating how European democracies fight coronavirus?” asked Latvian government advisor Ieva Ilves in an editorial highlighting the tension between state interests and multinational corporations.[48]

The converse situation also poses a risk: states can leverage their power over companies for outcomes neither intended nor desired by the businesses themselves—and in ways that harm individual rights. For example, developers of Thailand’s contact-tracing app, Mor Chana, withdrew from cooperation with the government in January 2021 following concerns that the program was not being implemented transparently or in ways that would serve the public interest.[49]

The social risks are compounded when governments collect datasets that are increasingly large and feature-rich. “Big data” can be especially helpful for improving tasks such as syndromic surveillance, when critical input variables—such as symptoms associated with a new illness—are not known at the outset. Yet massive, complex datasets also increase the capacity for data to be used beyond its initial purpose, which increases the risk of data misuse. For example, combining contact-tracing data with credit card activity offers granular information that could jeopardize civil liberties—and may not improve health outcomes, given that geolocation data does little to stem the pandemic in the absence of public health measures that provide more support to exposed persons.[50]

As many nations recalibrate public health needs amid vaccine rollouts, they will face long-term questions about how to adjust and dismantle the technology and surveillance infrastructures created to track Covid-19 exposure. The threat of “mission creep” and misappropriation of public health data is neither abstract nor speculative. In January 2021, the Singapore government acknowledged that data from TraceTogether could be accessed by law enforcement to support criminal investigations, despite earlier assurances that data would only be used if an individual tested positive.[51] The acknowledgement prompted public outcry and resulted in subsequent legislation that limits access to contact-tracing data to specific cases involving “serious offenses,” such as kidnapping or terrorism.[52] As the Singapore example demonstrates, surveillance infrastructures can be repurposed, thereby compounding the challenges of ensuring public- and private-sector accountability.

In mounting technological responses to the pandemic, state actors and private entities can serve as allies or opponents of individual rights, depending on the alignment of interests and needs. The global health crisis has generated new urgency to ensuring that configurations of public-private power continue to protect individual rights and the interests of vulnerable groups in particular.

VII. BUILDING A BETTER POST-PANDEMIC FUTURE

In the face of these challenges, some responses to the pandemic have also given reason for optimism. Crisis conditions can create opportunities to rethink the implicit and explicit social compact in ways that would allow societies to operate more effectively and more justly. While a one-size-fits-all approach will not accommodate the diversity of global privacy and public health needs, several basic principles and insights have emerged that can guide current and future health emergency responses. These insights vary in complexity and scale. Some are relatively short-term policy undertakings, while others require adopting new approaches to leadership and public trust. Nonetheless, they all hold promise for improving social resilience in the months and years ahead.

1) Renewal of Social Compacts

The pandemic has created an opportunity to rethink the social compacts that connect communities and underlie the legitimacy of governments. In many parts of the world, public trust in governments, regulatory agencies, and public health messaging has been eroded. Further, mistrust is unevenly distributed across different demographic groups and political orientations. For example, given well-established past and present abuses, some Black Americans have expressed understandable skepticism about scientific research and clinical medicine.[53] At times, communities mistrust authorities for good reason. However, distrust of information sources and a lack of shared facts threaten to undercut the effectiveness of public health initiatives, such as the rollout of vaccines.[54]

Moving forward, it is clear that, in creating a ‘new normal,’ societies can strive for more than simply repairing pre-existing social compacts. The crisis has created an opportunity to rethink processes of deliberation, collaboration, technology construction, and democratic governance to build more resilient societies. The principles and processes that emerge from such deliberation are likely to vary markedly depending on the society, its privacy context, its history, and its values. However, a commonality is that exceptional moments also create opportunities to build new architectures of trust—technical, institutional, and social—that increase inclusivity and social justice.

2) Consultation and Collaboration

Engaging in local consultation and cross-sector collaboration for the development of public health measures can support more responsible use of technology. A number of promising examples of local partnerships emerged in the early months of the pandemic. For example, the Societal Experts Action Network, a collaboration between the National Science Foundation and the National Academies of Sciences, Engineering, and Medicine in the United States, connected researchers with local decision-makers, such as a network of mayors and city officials, who greatly needed expert information to guide local policy. Likewise, in the United Kingdom, a group of scientists and researchers formed a nongovernmental network, the Independent Scientific Advisory Group for Emergencies (or SAGE), to offer reliable information to policymakers and the public.

"Exceptional moments also create opportunities to build new architectures of trust—technical, institutional, and social—that increase inclusivity and social justice."

While academics are accustomed to long-term research cycles and macro-level conclusions, government officials and policymakers often need much more granular, straightforward information to assess risks. Another working group that included scholars based at the Safra Center for Ethics and the Global Health Institute, both at Harvard University, developed a dashboard with a risk map and locally relevant data that could give policymakers tools to calibrate their public health interventions. Such partnerships underscore the importance of broadening community connections during the pandemic.

Another promising social model that emerged during the pandemic was a proliferation of mutual aid groups.[55] Thousands of mutual aid societies arose globally to do work that states are unable or unwilling to do. A scaffolded state, rather than a paternalistic one, could support the work of mutual aid groups by providing funds and other resources. However, these grassroots organizations were often created in the context of government dysfunction and a lack of trust in public institutions. Building capacity outside the government can also contribute to confusion by blurring lines between public and private functions and enable states to abdicate important social services.

Affected communities need to be involved as participants in the process of designing technologies and consulted about their use. Too often, the design of socially essential technologies proceeds as a top-down process: governments partner with companies; partners create product specifications; and technology companies build products and software. Users might play a role in downstream testing, but their perspectives do not necessarily inform the fundamental design of products and services.

Researchers and developers have called for changing the fundamental process of creating technologies. How can affected groups—marginalized communities in particular—become co-designers of critical technology? Scholars and practitioners have offered a range of models for more equitable design, and a basic principle is that its construction process needs to be consultative and collaborative from its inception and should involve oversight from the people on whom the technology will have the greatest impacts.[56]

As valuable as local empowerment is, another lesson from the pandemic is that it cannot substitute for clear, top-level political leadership, transparent information flows, and advance planning. High-level coordination is essential for aligning financial investments, policy change, information gathering, and medical responses, among other priorities. The absence of such leadership in many nations around the world has resulted in a great variety of community responses and local engagement, but the devastating death toll of the coronavirus lays bare that community engagement, on its own, is not enough.

3) Transparency

The principle of transparency is critical to the development of responsible data usage during a public health crisis. Historically, one way that technologists have promoted transparency has been by normalizing the publication of the source code for applications. However, revealing the source code for programs such as contact-tracing apps is not sufficient to inform the public about how the programs are actually used. For example, the Australian government released the source code for its COVIDSafe app. However, it has not released the server-side source code, which determines how app-generated data is processed, or the algorithm that winnows Bluetooth-generated contact data into “proximity data” that is legible to contact tracers. Transparency is not just a technical matter of making code visible. It also involves clear policies and accountable governance that can instill trust.

True verification of data usage also requires revealing the cloud software and the human processes of maintenance and updating the application. The organization App Assay, an independent technology monitoring group, is evaluating leading Covid-19 tracking apps to evaluate their security, privacy protections, and likely impacts on public health, among other impacts. Such a system of independent monitoring has the potential to keep public health technologies more accountable; however, it faces a number of challenges. For example, many apps release new versions every month, and some of the most popular apps update even more frequently.[57] Different versions can vary dramatically in functionality and impacts. Further, the absence of global standards on data privacy makes it challenging for such organizations to create uniform metrics for evaluating applications used in different countries.

Governments also play a role in ensuring transparency around data collection and usage. Historically, “informed consent” has been a foundational principle governing the ethics of data collection, research, and policy in many jurisdictions. However, the notion of informed consent becomes increasingly complex in the context of public health and surveillance. Getting consent from minors and ensuring that users are truly informed about data risks are among the challenges that governments as well as nongovernmental organizations, schools, and businesses must address. Despite these difficulties, a more transparent system is more likely to gain public trust, and a legal infrastructure that assures people about the privacy of their data is more likely to support the creation of technologies that can be effective in a public health crisis.[58]

4) Data Minimalism

Another principle that undergirds trusted technologies is a desire to be as "light" as possible: to collect the least amount of data required for public health efficacy and to set purpose limitations surrounding the use of that data. Minimalism should be a foundational principle in technology that could be used toward surveillance ends in order to limit the potential of negative effects and misuse.[59] UNICEF recently issued guidelines for collecting data from children, who are globally recognized as a vulnerable group, and one of the principles is the collection of the least amount of data necessary. Such principles can be useful in guiding the construction of health data platforms.[60]

As the health crisis abates, there is likely to be pressure within some governments to preserve the complex and costly data-collection machinery created in response to Covid-19. Setting strict purpose limitations to data that has been collected can help ensure that, even if parts of the digital architecture are preserved, individual rights are protected and data already collected will be less subject to misuse.

One strategy for minimizing incursions on privacy involves policies that create mandatory standards for the expiration of data. Requiring "sunset clauses" can reduce risks that crisis-era surveillance practices become normalized. Such policies also encourage policymakers to renew discussions about the use of surveillance technologies. In April 2020, the European Union published guidelines about maintaining data protections amid the pandemic, placing responsibility on leaders and developers to review data collections and ensure that data expires once the needs do not justify the risks of its retention.[61] Sunsetting can be accomplished through technological design. Programmers can create code that builds sunsetting into technological platforms by requiring the deletion of data after it expires.

5) Efficacy Criteria and Assessments

A major challenge associated with contact-tracing programs was that, in the hasty rollout of new technologies associated with a global health crisis, neither politicians nor technology makers established clear guidelines for evaluating the effectiveness of interventions or assessing the harms they could cause. Stakeholders had little sense of who could evaluate a technology's efficacy, based on what standards, and according to what timeline.

Lack of discussion around these points has prompted civil society and rights advocates to call for greater transparency and public deliberation about the criteria for evaluating Covid-related technologies, particularly in terms of their impacts on vulnerable populations.[62] Further discussion is needed, not only about what those standards are, but also the processes and timelines for determining them.

Ongoing assessment and proportionality testing—comparing the risks of a new technology with its social benefits—are additional strategies for minimizing unnecessary incursions on privacy and social freedoms. In the early months of the pandemic, many governments launched contact-tracing programs without long-term strategies for managing and dismantling them. By contrast, the Norwegian government periodically monitored the impacts of its digital contact-tracing program, Smittestopp. After one evaluation, it concluded that the risks to privacy and security were not proportionate with the value of the data it collected, and the program was suspended.[63] Such proportionality tests could provide a way to assess and monitor the efficacy and impacts of pandemic responses and strengthen public trust around technological interventions.

VIII. AREAS OF FURTHER INQUIRY

The pandemic has renewed the urgency of improving interdisciplinary, multisector, and transnational inquiry, as many of the core questions related to pandemic response and future public health planning require thinking beyond the traditional parameters of siloed fields. In particular, greater connections are needed to improve public health knowledge among technologists, scholars of technology and data, and policy advocates.

Researchers have a unique potential in the months and years ahead to help make sense of pandemic-related changes and give decision-makers the tools to create better policies. The research to-do list is vast. In order to equip the public with better understandings of the pandemic era, the following list identifies several particularly promising avenues of inquiry.

1) Understanding Technology in Crisis

What is the role of technology in shaping policy, particularly in dynamic situations like pandemics and responses to catastrophic events? How do we develop robust processes for answering questions with data, including the necessary multisector collaborations? Research is needed to evaluate the proliferation of technology-oriented responses that emerged at the height of the pandemic. Such investigations would also strengthen research partnerships among computer scientists, data specialists, and sociologists, for example, seeking collaboratively to understand connections between different information architectures and social responses.

2) Technology and the Nation State

What is the relationship between national sovereignty and data collection and analysis? How can states guarantee protection of individual rights, given that the private sector typically mediates data collection? Technology companies are largely unaccountable to democratic processes, and this lack of accountability raises questions about whether companies have the legitimacy to intervene in global public health crises without additional regulatory constraints and governance structures. Pandemic-related partnerships between the public and private sectors have also raised questions about national security vulnerabilities and the ultimate ownership of sensitive health data. This research agenda would consider the relationships among different legal jurisdictions, transnational corporate structures, nationalist sentiment, and technology.

Emerging research is beginning to investigate different national strategies for responding to the crisis and assess the effectiveness of various policies. One such study led by researchers at Harvard, Cornell, and Arizona State Universities compares Covid-19 responses across different countries and classifies the outcomes in terms of control, consensus, or chaos.[64] Such research could better prepare future decision-makers to understand the tradeoffs and implications of different interventions.

3) Crisis, Trust, and Inequality

The impacts of the pandemic on poor and vulnerable communities will likely continue and possibly even intensify in the coming months, in terms of job losses, lack of access to medical care, and food insecurity. In many parts of the world, vulnerable communities have legitimate and long-standing reasons for distrusting political authorities. What policy and community responses best protected marginalized groups during the pandemic? This research agenda would shed light on the economic dimensions of the public health crisis and its disproportionate impact on different demographic groups. Research is also required that interrogates the relationship between technological surveillance and community trust, as well as the role technology plays in reinforcing or diminishing trust in public institutions.

4) Privacy after the Pandemic

An unprecedented amount of health data is now collected by and shared between private platforms. How can we ensure privacy protections and safeguard individual rights while promoting effective health policy and equitable health outcomes? Can those protections enable the sharing of enough information to mitigate public health risks? This line of inquiry would illuminate the underlying assumptions in the presumed tensions among protecting public health, preserving privacy, and ensuring equity.

5) Mapping Networks of Collaboration

What platforms or networks are needed to deepen work and strengthen collaboration among public health experts, social researchers, technologists, and civil liberties and human rights organizations? Around the world, new partnerships and networks emerged to fill voids in policymaking and threat assessments. Even as political tensions escalated between nations such as the United States and China, greater international collaboration and information exchange was needed to implement effective responses to a global crisis like Covid-19. Researchers can shed light on the processes for increasing coordination at the international, regional, and local levels by developing an observatory to map what is transpiring across varied locations as the foundation for diagnostic and prescriptive research.

The pandemic has also created opportunities to reshape and rethink coordination between academics and key decision-makers. In many instances, mismatches in the timescale of research, institutional priorities, and funding impeded coordination between researchers and policymakers. New collaboration could involve changing the timeframes and objectives of research and making deliverables more accessible to a wider range of audiences.

IX. CONCLUSION

The Social Science Research Council is committed to ongoing deliberation and research into the social impacts of Covid-19 by working with the Public Health, Surveillance, and Human Rights Network and other forums. From climate change to interconnected supply chains, communities around the world face new and often shared vulnerabilities to social shocks. Because the frequency of these shocks is expected to increase in the years ahead, the Council seeks to stimulate needed discussion and research about how to improve social resilience. This report provides analysis, principles, and directions for future inquiry that can guide the next phases of pandemic responses, vaccine administration, and post-pandemic planning. It is predicated on the hope that knowledge about past crises can better inform societies' responses to future emergencies. And it is motivated by the imperative that technological surveillance, social safety, and democratic rights must be balanced to preserve the well-being of all members of society.

ENDNOTES

[1] The report also benefited from the participation and insights of PHSHR Network members Henri Hammond-Paul and Beth Simone Noveck of GovLab, who collaborated with the Inter-American Bank to provide perspectives on Covid-19 in Latin America and the Caribbean. See Henri Hammond-Paul, Victoria Alsina-Burgues, Beth Simone Noveck, Valeria Palacios, and Frederico Levy, ***Smarter Crowdsourcing in the Age of Coronavirus: A Handbook of Innovative Political and Technical Proposals, and a Guide to Their Implementation*** (New York: GovLab, New York University, February 2021).

[2] Adam Przeworski, "**COVID-19 Reveals the Fragility of Our Values**," *The Global*, June 16, 2020.

[3] See, for example, Matthew Mohan, "**Singapore Police Force Can Obtain TraceTogether Data for Criminal Investigations: Desmond Tan**," *Channel News Asia*, January 4, 2021; Zack Whittaker, "**Australia's Spy Agencies Caught Collecting COVID-19 App Data**," *TechCrunch*, November 24, 2020; "**German Restaurants Object after Police Use COVID Data for Crime-Fighting**," *Reuters*, July 31, 2020.

[4] Eileen Yu, "**Singapore to Begin Nationwide Distribution of COVID-19 Contact Tracing Wearables**," *ZDNet*, September 9, 2020.

[5] Brian J. Kim, "**South Korea Has the Legal Infrastructure to Fight Pandemics; The US Doesn't**," *GlobalAsia*, March 30, 2020.

[6] Seung-Youn Oh, "**South Korea's Success Against COVID-19**," *Regulatory Review*, May 14, 2020.

[7] "**COVID-19 Dashboard by the Center for Systems Science and Engineering (CSSE) at Johns Hopkins**," Johns Hopkins University and Medicine, accessed January 20, 2021.

[8] In contrast to these early testing measures, South Korea has not adopted as widespread a usage of testing as many other nations have as the pandemic unfolded. Cumulatively, South Korea has performed only a small number of tests relative to its population: as of January 2021, it had performed roughly 10 tests for every 100 people, as compared to nearly 90 tests for every 100 people in the United States, where the virus has still not been contained. "**COVID-19 Dashboard by the Center for Systems Science and Engineering (CSSE) at Johns Hopkins**," Johns Hopkins University and Medicine, accessed January 20, 2021. See also Sangchul Park, Gina Jeehyun Choi, and Haksoo Ko, "**Information Technology–Based Tracing Strategy in Response to COVID-19 in South Korea—Privacy Controversies**," *JAMA* 323, no. 21 (April 2020): 2129–2130; Kyung Sin Park, "**Korea's COVID-19 Success and Mandatory Phone Tracking**," *Open Net Korea*, October 20, 2020.

[9] A significant part of the civil society has joined in filing a constitutional challenge against the nonconsensual, nonjudicial aspect of data collection. Kyung Sin Park, "**Location Tracking of COVID-19 Patients and Location Monitoring of Quarantined Must Conform To Human Rights Principles**," *Open Net Korea*, April 10, 2020. See also Eun A Jo, "**South Korea's**

Experiment in Pandemic Surveillance," *The Diplomat*, April 13, 2020.

[10] See, for example, Gyuwon Jung, Hyunsoo Lee, Auk Kim, and Uichin Lee, "Too Much Information: Assessing Privacy Risks of Contact Trace Data Disclosure on People With COVID-19 in South Korea," *Front Public Health* 8, no. 305 (2020); Woosung Hwang, "COVID-19 in South Korea: Privacy and Discrimination Concerns," *Bill of Health*, Harvard Law School, Petrie-Flom Center, June 9, 2020.

[11] Oh, "South Korea's Success."

[12] Reports of police violence in enforcing lockdowns has emerged from, inter alia, South Africa, Nigeria, Uganda, Kenya, Zimbabwe, Kenya, and Burkina Faso. See, generally, Richard Youngs and Elene Panchulidze, ***Global Democracy & COVID-19: Upgrading International Support*** (Stockholm, Sweden: International Institute for Democracy and Electoral Assistance, 2020); Eda Seyhan, "The Other Death Toll from the Coronavirus Pandemic," Al Jazeera, May 2, 2020. For specific cases, see, for example, Claire-Anne Lester, "Who Will Watch the Watchmen?" *Africa Is a Country*, April 6, 2020 (South Africa); Marianne Merten, "Lockdown Level 3, Version 3: Policymaking on the Hoof amid War Talk," *Daily Maverick*, July 17, 2020 (South Africa); "The Bullet and the Virus: Police Brutality in Kenya's Battle against Coronavirus," *BBC News Africa*, June 15, 2020 (Kenya); and Joyce Abalo and Sarah O'Sullivan, "Ugandans Brace for the Worst," *Africa Is a Country*, April 3, 2020 (Uganda).

[13] Amy Maxmen, "Ebola Prepared These Countries for Coronavirus—But Now Even They Are Floundering," *Nature*, July 21, 2020.

[14] Guthrie S. Birkhead, Michael Klompas, and Nirav R. Shah, "Uses of Electronic Health Records for Public Health Surveillance to Advance Public Health," *Annual Review of Public Health* 36, no. 1 (2015): 345–359.

[15] Christina Farr, "These 'Disease Hunters' Developed a Novel Technique for Tracking Pandemics after 9/11, But Lost Funding Right before COVID-19," CNBC, April 4, 2020.

[16] For more on NSSP, see "How NSSP Works Across CDC," Centers for Disease Control and Prevention, accessed September 30, 2020. For critiques of the US federal response to Covid-19, see, for example, Philip Wallach and Justus Myers, ***The Federal Government's Coronavirus Response—Public Health Timeline*** (Washington, DC: Brookings Institution, March 2020); Alexis C. Madrigal and Robinson Meyer, "How the Coronavirus Became an American Catastrophe," *The Atlantic*, March 21, 2020.

[17] Samrachana Adhikari, Nicholas P. Pantaleo, Justin M. Feldman, Olugbenga Ogedegbe, Lorna Thorpe, and Andrea B. Troxel, "Assessment of Community-Level Disparities in Coronavirus Disease 2019 (COVID-19) Infections and Deaths in Large US Metropolitan Areas," *JAMA Network Open*, July 28, 2020.

[18] "Why Have Black and South Asian People Been Hit Hardest by COVID-19?" Office for National Statistics, December 14, 2020.

[19] "COVID-19 Will Double Number of People Facing Food Crises Unless Swift Action Is Taken," UN World Food Program, April 21, 2020; Peter S. Goodman, Abdi Latif Dahir, and

Karan Deep Singh, “The Other Way Covid Will Kill: Hunger,” *New York Times*, September 11, 2020.

20 Maria Godoy and Daniel Wood, “What Do Coronavirus Racial Disparities Look Like State By State?” *NPR*, May 30, 2020.

21 Michele Gilman and Rebecca Green, “The Surveillance Gap: The Harms of Extreme Privacy and Data Marginalization,” *N.Y.U. Review of Law & Social Change* 42 no. 2 (2018).

22 Laura Silver, *Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally* (Washington, DC: Pew Research Center, February 5, 2019); Piotr Sapiezynski, Johanna Pruessing, and Vedran Sekara, “The Fallibility of Contact-Tracing Apps,” *arXivLabs*, May 22, 2020.

23 Saira Asher, “TraceTogether: Singapore Turns to Wearble Contact-Tracing Covid Tech,” *BBC News*, July 4, 2020.

24 “Is TraceTogether Mandatory?” TraceTogether, September 8, 2020; Balli Kaur Jaswal, “Rise in Coronavirus Cases Brings to Light Singaporeans’ Racist Attitudes Towards Foreign Workers,” *South China Morning Post*, April 23, 2020.

25 Mark Latonero, “Stop Surveillance Humanitarianism,” *New York Times*, July 11, 2019.

26 Fergus Ryan, “Mobile Phone Data Help Contain Human Spread of Malaria,” *Financial Times*, April 24, 2016.

27 Ryan, “Mobile Phone Data.”

28 Nic Fildes and Javier Espinoza, “Tracking Coronavirus: Big Data and the Challenge to Privacy,” *Financial Times*, April 8, 2020.

29 Jo Becker, “This Contact Tracer Is Fighting Two Contagions: The Virus and Fear,” *New York Times*, August 9, 2020.

30 Danielle Allen, Lucas Stanczyk, I. Glenn Cohen, Carmel Shachar, Rajiv Sethi, Glen Weyl, and Rosa Brooks, *Securing Justice, Health, and Democracy against the COVID-19 Threat* (Cambridge, MA: Edmond J. Safra Center for Ethics, Harvard University, 2020).

31 Lawrence O. Gostin and Lindsey F. Wiley, “Governmental Public Health Powers During the COVID-19 Pandemic: Stay-at-Home Orders, Business Closures, and Travel Restrictions,” *JAMA* 323, no. 21 (2020).

32 Tedros Adhanom Ghebreyeses, “Health Is a Fundamental Human Right,“ World Health Organization, December 10, 2017.

33 “Police Fine 1,300 for Breaking Virus Rules; Official: Only 8 Test Results Wrong,” *Times of Israel*, March 28, 2020.

34 Johnny Diaz, “KFC Birthday Party Costs $18,000 in Covid-19 Fines in Australia,” *New York Times*, July 11, 2020.

35 Caitlin O’Kane, “Poland Is Making Quarantined Citizens Use a Selfie App to Prove They’re Staying Inside,” *CBS News*, March 23, 2020.

36 Hyonhee Shin, “South Korea Warns of Deportation, Jail for Quarantine Violators,” *Reuters*, March 25, 2020.

[37] Allen et al., *Securing Justice*.
[38] Karen Lema and Neil Jerome Morales, "Philippines to Use Police in House-to-House Searches for COVID-19 Cases," *Reuters*, July 14, 2020.
[39] Julie McCarthy, "Why Rights Groups Worry About the Philippines' New Anti-Terrorism Law," *NPR*, July 21, 2020; Jeremiah Joven B Joaquin and Hazel T Biana, "Philippine Crimes of Dissent: Free Speech in the Time of COVID-19," *Crime Media Culture*, July 30, 2020.
[40] "20 Years in Jail for Spreading Fake Coronavirus News," *The Standard*, March 29, 2020.
[41] Laetitia Bader, "Millions of Ethiopians Can't Get COVID-19 News," Human Rights Watch, March 20, 2020; CIPESA (@cipesaug), "#Guinea: The Country Went to the Polls This Past Weekend for a Referendum," Twitter, March 23, 2020; Yi-Ling Liu, "In China, GitHub Is a Free Speech Zone for Covid Information," *Wired*, September 9, 2020.
[42] Natalia Zviagina, quoted in "Russia's Use of Facial Recognition Challenged in Court," *BBC*, January 31, 2020; Gregory Barber, "Schools Adopt Face Recognition in the Name of Fighting Covid," *Wired*, November 3, 2020.
[43] See, for example, Sabrina Tavernise, "Texas and Ohio Include Abortion as Medical Procedures That Must Be Delayed," *New York Times*, March 23, 2020.
[44] Azi Paybarah, "Protesters Say the Police Use Social Distancing to Justify Crackdown," *New York Times*, May 5, 2020.
[45] Steven Feldstein, "The Global Expansion of AI Surveillance" (working paper, Carnegie Endowment for International Peace, Washington, DC, September 17, 2019).
[46] Ulises Ali Mejias and Nick Couldry, "Resistance to the New Data Colonialism Must Start Now," *Al Jazeera*, April 29, 2020. See also Michael Kwet, "Digital Colonialism: US Empire and the New Imperialism in the Global South," *Race & Class* 60, no. 4 (2019): 3–26.
[47] Steven Melendez, "North Dakota's COVID-19 App Has Been Sending Data to Foursquare and Google," *Fast Company*, May 21, 2020.
[48] Ieva Ilves, "Why Are Google and Apple Dictating How European Democracies Fight Coronavirus?" *The Guardian*, June 16, 2020.
[49] Mongkol Bangprapa and Komsan Tortermvasana, "Govt Denies Rift with Mor Chana Creators," *Bangkok Post*, January 19, 2021.
[50] On the limitations of Bluetooth and geolocation technology, see Patrick Howell O'Neill, "Bluetooth Contact Tracing Needs Bigger, Better Data," *MIT Technology Review*, April 22, 2020.
[51] Ellen Yu, "Singapore Police Can Access COVID-19 Contact Tracing Data for Criminal Investigations," *ZDNet*, January 4, 2021.
[52] Ellen Yu, "Singapore Passes Bill Governing Police Use of Contact Tracing Data," *ZDNet*, February 3, 2021.
[53] See, for example, Cary Funk, Brian Kennedy, and Alec Tyson, "Black Americans Have Less Confidence in Scientists to Act in the Public Interest," *Fact Tank*, Pew Research Center, August 28, 2020.

[54] "New Poll Finds BAME Groups Less Likely to Want COVID Vaccine," Royal Society for Public Health, December 16, 2020.

[55] Robert Soden, "Crisis Informatics and Mutual Aid during the Coronavirus Pandemic: A Research Agenda," *Items*, Social Science Research Council, July 2, 2020.

[56] See, for example, Sasha Costanza-Chock, ***Design Justice: Community-Led Practices to Build the Worlds We Need*** (Cambridge, MA: MIT Press, 2020); Christina N. Harrington, "Towards Equitable Design When We Design with Marginalized Communities," *Medium*, September 18, 2019.

[57] See, for example, Dmitry Garbar, "How Often Should You Update Your Mobile App?" *Apptentive*, December 27, 2018.

[58] Jessica Rich, "How Our Outdated Privacy Laws Doomed Contact-Tracing Apps," *TechTank*, Brookings Institution, January 28, 2021.

[59] The GDPR uses the concept of "data minimization" to refer to the practice of collecting and using only the data required for an intended purpose. Data minimalism incorporates this but additionally points to technical and normative processes through which it can be accomplished.

[60] "Industry Toolkit: Children's Online Privacy and Freedom of Expression," United Nations Children's Fund, May 2018.

[61] "Covid-19 Tracing Apps: Ensuring Privacy and Data Protection," *Modern Diplomacy*, May 7, 2020.

[62] See, for example, "Government Must Publish Evidence That the Contact Tracing App Works and Will Not Fail Those Most at Risk of COVID-19," press release, Health Foundation, September 23, 2020.

[63] See, for example, Natasha Lomas, "Norway Pulls Its Coronavirus Contacts-Tracing App after Privacy Watchdog's Warning," *TechCrunch*, June 15, 2020.

[64] Sheila Jasanoff, Stephen Hilgartner, J. Benjamin Hurlbut, Onur Özgöde, and Margarita Rayzberg, ***Comparative Covid Response: Crisis, Knowledge, Politics*** (Futures Forum on Preparedness, January 12, 2021). For information about the project, see also: https://www.futuresforumonpreparedness.org/research.

MANUAL CONTACT TRACING

[I] Vi Hart et al., “Outpacing the Virus: Digital Response to Containing the Spread of COVID-19 While Mitigating Privacy Risks“ (COVID-19 White Paper 5, Edmond J. Safra Center for Ethics, Harvard University, Cambridge, MA, April 3, 2020).
[II] Ed Shanahan, “Party Guests Wouldn’t Talk After 9 Tested Positive. Then Subpoenas Came,“ *New York Times*, July 1, 2020.
[III] Roger Doughty, “The Confidentiality of HIV-Related Information: Responding to the Resurgence of Aggressive Public Health Interventions in the AIDS Epidemic,“ *California Law Review* 82, no. 1 (1994): 111–184.
[IV] Doughty, “The Confidentiality.“
[V] Shanahan, “Party Guests.“

DIGITAL CONTACT TRACING

[VI] Dimitri Tokmetzis and Morgan Meaker, “We Were Told Technology Would End Covid-19 Lockdowns, but the Truth Is There’s No App for That,“ *The Correspondent*, May 31, 2020.

GLOBAL PRIVACY NORMS

[VII] UN General Assembly, Resolution 217 A (III), Universal Declaration of Human Rights (December 10, 1948); UN General Assembly, Resolution 68/167, The Right to Privacy in a Digital Age, A/RES/68/167 (December 18, 2013).
[VIII] I. Glen Cohen and Michelle M. Mello, “HIPAA and Protecting Health Information in the 21st Century,” *JAMA* 320, no. 3 (2018): 231–232; Arellano et al., “Privacy Policy.”
[IX] Leslie P. Francis and John G. Francis, “Informatics and Public Health Surveillance,” in *Bioinformatics Law: Legal Issues for Computational Biology in the Post-Genome Era*, ed. Jorge L. Contreras and A. James Cuticchia (Chicago: American Bar Association, 2013).
[X] See, for example, Scott Warren, “New Amendments Passed to Japan’s Data Privacy Law,” *National Law Review*, August 19, 2020; Arindrajit Basu and Justin Sherman, “Key Global Takeaways From India’s Revised Personal Data Protection Bill,” *Lawfare*, January 23, 2020.
[XI] See, for example, Emmanuel Pernot-Leplay, “China’s Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?” *Pennsylvania State Journal of Law & International Affairs* 8, no. 1 (2020).

PUBLIC HEALTH, SURVEILLANCE, AND HUMAN RIGHTS NETWORK

Joseph Ali
Assistant Professor and Associate Director for Global Programs, Berman Institute of Bioethics
Johns Hopkins University

Joe Amon
Clinical Professor and Director of the Office of Global Health, Dornsife School of Public Health
Drexel University

Matthias Bäcker
University Professor and Chair of Public Law
Johannes Gutenberg University Mainz

Natalie Banner
Understanding Patient Data Lead
Wellcome Trust

Jason Bay
Senior Director (Government Digital Services)
GovTech Singapore

Khadine Bennett
Director of Advocacy and Intergovernmental Affairs
ACLU of Illinois

Sutawan Chanprasert
Founder
DigitalReach

Andrew Chen
Research Fellow, Koi Tū: The Centre for Informed Futures
University of Auckland

Joshua Cohen
Faculty; Distinguished Senior Fellow in Law, Philosophy and Religion
Apple University; University of California

Emma Day
Human Rights Lawyer and Child Protection Consultant
UNICEF East Asia & Pacific Regional Office

Ronald Deibert
Professor of Political Science and Director, Citizen Lab
University of Toronto

Lilian Edwards
Professor of Law and Chair of Law, Innovation and Society
Newcastle University

Johannes Ernst
President and CEO
Indie Computing Corp.

Camille François
Chief Innovation Officer
Graphika

Sharon Bradford Franklin
Policy Director, Open Technology Institute
New America

Urs Gasser
Professor of Practice and Executive Director, Berkman Klein Center for Internet & Society
Harvard University

Gregg Gonsalves
Professor of Epidemiology
Yale University

Graham Greenleaf
Professor of Law & Information Systems
University of New South Wales

Jeffrey Kahn
Andreas C. Dracopoulos Director of the Johns Hopkins Berman Institute of Bioethics
Johns Hopkins University

Amy Kapczynski
Professor of Law
Yale University

Sir David King
Founder and Chair, Centre for Climate Repair
University of Cambridge

Christopher Kirchhoff
Senior Fellow
Schmidt Futures

Mark Latonero
Senior Associate
Center for Strategic and International Studies

Fredrik Liljeros
Professor of Sociology
Stockholm University

Mary Madden
Senior Fellow
Joan Ganz Cooney Center

Alondra Nelson
President
Social Science Research Council

Beth Simone Noveck
Chief Innovation Officer
State of New Jersey

Kyung Sin Park
Professor of Law and Executive Director, opennetkorea.org
Korea University

Frank Pasquale
Professor of Law
Brooklyn Law School

Sobia Raza
Senior Fellow
The Health Foundation

Stephen Reicher
Bishop Wardlaw Professor
University of St. Andrews

Hilary Ross
Senior Program Manager, Assembly: Disinformation Program
Harvard University

Piotr Sapieżyński
Associate Research Scientist, Khoury College of Computer Sciences
Northeastern University

Nicole Triplett
Director of Policy
Data for Black Lives

Stefaan Verhulst
Co-Founder and Chief Research and Development Officer, Governance Laboratory
New York University

Jonathan Zittrain
George Bemis Professor of International Law, Co-Founder and Director, Berkman Klein Center for Internet & Society
Harvard University

APPENDIX

The Social Science Research Council provided the following research briefings on surveillance issues related to the pandemic to members of the Public Health, Surveillance, and Human Rights Network to inform their discussions:

Primer I | Some Considerations on the Surveillance and Rights Continuum

Primer II | On Privacy and Contact Tracing

Primer III | Rights, Law, and Technology in the State of Emergency—Three Cases

Primer IV | Technology, Surveillance and Rights in Africa during Covid-19

Primer V | Health Data Privacy and Covid-19

ACKNOWLEDGMENTS

The Social Science Research Council gratefully acknowledges the following staff members, who played an indispensable role in the Public Health, Surveillance, and Human Rights Network's convenings and the development of this report:

David A. Banks, Associate Research Advisor, Public Health, Surveillance, and Human Rights Network

Alexa Dietrich, Program Director, Scholarly Borderlands and Religion and the Public Sphere

Rebecca Tave Gluskin, Chief Statistician and Deputy Director, Measure of America

Clara Hanson, Associate Research Advisor, Public Health, Surveillance, and Human Rights Network

Ronald Kassimir, Vice President of Programs

Renee King, Associate Research Advisor, Public Health, Surveillance, and Human Rights Network and Measure of America

Duncan Omanga, Program Officer, African Peacebuilding Network

Michael Miller, Program Director, Just Tech and Media & Democracy

Vina Tran, Chief of Staff

In addition to the SSRC staff members listed above, Juni Ahari, Cole Edick, Line Sidonie Talla Mafotsing, Clare McGranahan, Rajat Singh, and Zach Zinn contributed to the administrative, communications, and web development efforts behind this publication.

Over the course of the network's discussions, leading scholars and researchers delivered presentations to members on topics of central concern to this report. We extend our thanks to the following guest speakers, who lent their time and expertise to inform the work and conversations of the PHSHR Network:

Danielle Allen, James Bryant Conant University Professor and Director of the Edmond J. Safra Center for Ethics, Harvard University

Alvaro Bedoya, Professor and Founding Director of the Center on Privacy and Technology, Georgetown University School of Law

Pauline Byakika-Kibwika, Chair of the Department of Medicine, Makerere University College of Health Sciences

Josh Platzky Miller, Affiliated Lecturer in the Centre of Development Studies, University of Cambridge

Sharath Srinivasan, Co-Director of the Centre of Governance and Human Rights, David and Elaine Potter Lecturer in the Department of Politics and International Studies, and Fellow of King's College, University of Cambridge

We are grateful to Mary Bridges, who provided editorial support for this report, and Beth Post and Michael Shaw, who oversaw the design.

For nearly a century, the Social Science Research Council has acted as a trusted intermediary connecting academic disciplines, universities, government organizations, NGOs, and world regions. We operate independently of any university affiliation or partisan interest, and our ability to serve as both a platform for launching research and a producer of knowledge makes the Council uniquely able to raise the bar for social science inquiry. Across our many activities—which range from providing fellowships to publishing books to organizing United Nations briefings to building online knowledge resource platforms—our mission is to mobilize scholars and social knowledge to build a more just and democratic world.

Please support the work of the Social Science Research Council. Contributions allow us to support scholars, launch innovative research programs, strengthen networks across disciplines, and seek solutions to today's most pressing questions.

www.ssrc.org/donate

SSRC

SOCIAL SCIENCE RESEARCH COUNCIL

One Pierrepont Plaza | Floor 15 | Brooklyn, NY 11201
(212) 377-2700 | www.ssrc.org