DECISIONS, DECISIONS, DECISIONS.

Responsible Business Decision-Making Before, During, and After Public Health Emergencies: A Rights-Based Approach to Technology and Data Use

DECEMBER 2020

BSR®
The Business of a Better World

About This Report

This paper sets out the key elements of a human rights-based approach to the use of data and technology solutions during public health emergencies in today and tomorrow's digital era, with a focus on the role of business and impacts on privacy.

The paper pays special attention to how different human rights objectives can be achieved at the same time, to the relationship between the state duty to protect human rights and the corporate responsibility to respect human rights, and to the norms, principles, and standards that may need to last beyond the duration of COVID-19.

The core of this paper is a framework to guide businesses through human rights-based decision making during public health emergencies. The framework is informed by a combination of international human rights law related to states of emergency, allowable limitations and derogations of rights, relevant regulations, standards, and principles grounded in human rights, and lessons learned from past emergencies.

ACKNOWLEDGEMENTS

This report was researched and written by Lindsey Andersen, Dunstan Allison-Hope, Susan Morgan, Lale Tekisalp, and Jenny Vaughan at BSR. BSR wishes to thank all Microsoft employees, stakeholders, and subject matter experts who participated in this research.

This paper was funded by Microsoft, though BSR retained full editorial control over its contents.

DISCLAIMER

BSR publishes occasional papers as a contribution to the understanding of the role of business in society and the trends related to corporate social responsibility and responsible business practices. BSR maintains a policy of not acting as a representative of its membership, nor does it endorse specific policies or standards. The views expressed in this publication are those of its authors and do not necessarily reflect those of BSR members. BSR's papers contain preliminary research, analysis, findings, and recommendations; they are circulated to stimulate timely discussion and critical feedback and to influence ongoing debate on emerging issues.

Contents

Executive Summary 3

Introduction 6

A Human Rights-Based Framework for Business Decisions 9

Data Use and Privacy in Global Health Emergencies 15

Foundations for a Human Rights-Based Approach 21

Understanding Public Health Emergencies 30

Recommendations 34

COVID-19 Case Studies and Lessons Learned from Past Emergencies 37

Conclusions and Areas for Further Enquiry 42

Executive Summary

The COVID-19 public health emergency has surfaced important questions about the relationship between the right to privacy and other rights, such as the right to health, work, movement, expression, and assembly. Data and technology solutions can be used for many positive outcomes, such as facilitating "back to work" efforts, enhancing research into COVID-19 vaccines and treatments, and allowing the resumption of economic activity while also protecting public health.

However, these uses can also involve the infringement of privacy rights and new forms of discrimination, and cause harm to vulnerable groups. Some governments are using the pandemic as an excuse to expand their power, and there is widespread concern that efforts to address COVID-19 could become a more permanent form of surveillance.

As the providers of data and digital infrastructure[1], technology companies will often be central in public health emergency response efforts. We believe that companies have an opportunity to take actions that promote the enjoyment, realization, and fulfillment of human rights, including the right to health and science. Companies also have a responsibility under the UN Guiding Principles on Business and Human Rights (UNGPs) to identify, prevent, and mitigate human rights harms in which they are involved, and this does not disappear or relax in times of emergency.

Moreover, although COVID-19 may be the first truly global pandemic of the modern age, it will not be the last—in fact, experts expect that pandemics will become increasingly common. Lessons learned about business and human rights during the COVID-19 must be captured, while recognizing that future public health emergencies may be different than this one.

A HUMAN RIGHTS FRAMEWORK FOR DECISION MAKING

This paper sets out the key elements of a human rights-based approach to the use of data and technology solutions during public health emergencies in today's digital era, with a focus on the role of business and impacts to privacy.

The paper pays special attention to how different human rights objectives can be achieved at the same time, to the relationship between the state duty to protect human rights and the corporate responsibility to respect human rights, and to the norms, principles, and standards that may need to last beyond the duration of COVID-19.

The core of this paper is a framework for businesses that can act as a guide through human rights-based decision making during public health emergencies. The framework is informed by a combination of international human rights law related to states of emergency, allowable limitations and derogations of rights, relevant regulations, standards and principles grounded in human rights, and lessons learned from past emergencies.

A summary of this framework can be found on page 5 and the full version on page 10.

[1] Digital infrastructure is what enables the creation and operation of technology solutions. Cloud platforms and operating systems are critical components of digital infrastructure provided by technology companies.

RECOMMENDATIONS FOR COMPANIES

This paper makes the following recommendations for companies to help ensure they take rights-respecting approaches to future public health emergencies.

ACT: WHAT COMPANIES SHOULD DO INTERNALLY

- Make business decisions during public health emergencies using a human rights-based framework.
- Avoid known pitfalls by deliberating on the right solution, working only with the appropriate government authorities, setting up effective escalation processes, and setting time limits or sunset clauses in contracts with the government.

ENABLE: HOW COMPANIES SHOULD WORK WITH OTHERS

- Be as transparent as possible. This includes contract transparency, transparency about what kinds of data are being used and how, the privacy protections in place, any redlines or principles guiding decisions, and maintaining records for system audits.
- Ensure all appropriate stakeholders are at the table, including public health authorities and experts, civil society, and members of vulnerable groups, among others.
- Engage with other companies to establish rights-based redlines and set standards.
- Carefully engage and educate government customers to avoid scope creep and misuse or abuse of a product, service, or data sharing arrangement.
- Pursue partnerships to proactively advance public health.

INFLUENCE: HOW COMPANIES SHOULD INFLUENCE PUBLIC POLICY

- Advocate for rights-respecting approaches to dealing with public health emergencies.
- Challenge governments when required to share data beyond what is legitimate, necessary, and proportionate.

CONCLUSIONS

We expect a future with more public health emergencies and greater company involvement in addressing them. In this context, companies should be prepared to make human rights-based business decisions in the complicated context of public health emergencies to avoid unduly infringing on other human rights in the name of protecting public health, and to prevent invasive emergency measures from becoming permanent. The ideas discussed in this paper and the human rights framework for business decisions in public health emergencies are one contribution toward that end.

However, several questions and challenges remain that merit further exploration: (1) securing more evidence of which technology and data-based solutions work and which do not; (2) exploring the extent to which emergency measures are needed to address public health crises; (3) better understanding the link between privacy and other human rights; and (4) creating new frameworks for the role of companies in promoting the enjoyment, realization, and fulfillment of human rights, over and above company responsibilities under the UN Guiding Principles on Business and Human Rights (UNGPs).

SUMMARY

A Human Rights Framework for Business Decisions in Response to Public Health Emergencies

Does the activity involve limiting rights or can a fully rights-respecting approach be taken?
If limits are needed, are they allowed under the International Covenant on Civil and Political Rights (ICCPR), International Covenant on Economic, Social and Cultural Rights (ICESCR), or do they require derogation of rights based on emergency powers?

Are the limitations on rights consistent with international human rights principles?
These principles are necessity, proportionality, provided for by law, non-discrimination, and based on science.

Is the activity consistent with the core obligations of the rights to health and science?
These obligations are based on the principles of availability, accessibility, acceptability, and quality.

Does the activity comply with relevant privacy and general data or health data regulations?
Notable examples include the General Data Protection Regulation (GDPR) in the European Union and the Health Insurance Portability and Accountability Act (HIPAA) in the USA.

Will the activity follow other best practices for technology and data use in a public health emergency?
These best practices include transparency, time-bound, consent, voluntary, data minimization, access limitation, fairness, safeguarded from commercial interest, accountability, stakeholder participation, efficacy, non-punitive.

Can the contract include prohibited uses to enable the company to challenge misuse / abuse and terminate the agreement if necessary?
For example, this may include prohibiting the use of data by specified government agencies, or having the ability to report concerns to the World Health Organization (WHO), civil society, or other interested parties.

1. Introduction

The COVID-19 public health emergency has surfaced important questions about the relationship between the right to privacy and the fulfillment of other rights, such as the rights to health, work, movement, expression, and assembly. There is significant interest in how data and technology solutions can be used for positive outcomes, such as facilitating “back to work” efforts, enhancing research into COVID-19 vaccines and treatments, and allowing resumption of economic activity while also protecting public health.

However, these uses have been accompanied by concerns that privacy rights may be violated, that new forms of discrimination may arise, and that vulnerable groups may be especially susceptible to harm. There are also fears that governments may use the pandemic as an excuse to expand their power.

Companies providing products or services to those governments could find themselves enabling encroachments on privacy beyond what is necessary to address COVID-19, and that may lead to the entrenchment of surveillance states and the long-term restriction of rights.

TRADITIONAL HUMAN RIGHTS PRINCIPLES IN MODERN HEALTH EMERGENCIES

We believe that companies and government authorities should use data and digital infrastructure in the service of public health, while also addressing the human rights risks inherently involved in widespread data collection, analysis, and transfer. They should also be conscious of potential future impacts.

There are various human rights-based norms, principles, and standards that can help navigate a pathway through these dilemmas.

For example, Article 4 of the International Covenant on Civil and Political Rights (ICCPR) and its accompanying General Comment 29 allow governments to derogate from specified human rights during times of public emergency, provided that such measures are consistent with their other obligations under international law and do not involve discrimination solely on the ground of race, color, sex, language, religion, or social origin. The Siracusa Principles, adopted by the UN Economic and Social Council in 1984, describe limitations on the restriction of human rights that governments may apply for reasons of public health or national emergency.

However, three factors are challenging the application of these principles in modern day practice:

- **Changes in the digital realm:** Ever-more-powerful computing, massive growth in the availability of data, increasingly sophisticated artificial intelligence capabilities, and the centrality of digital infrastructure in everyday life have transformed the opportunities and risks associated with the use of digital technologies for public health.

- **Increased involvement of companies:** These principles were written for governments rather than companies, yet today the private sector has a far more significant role and power in the fulfillment of human rights than when the principles were drafted.

- **Complexities of a global pandemic:** These principles were not written to address the complexities of a global pandemic, and new insights about their implementation are emerging in real time.

We believe that companies have an opportunity to take actions that promote the enjoyment, realization, and fulfillment of human rights, including the right to health and science, through the use of technology and data during times of public health emergency.

Companies also have a responsibility under the UN Guiding Principles on Business and Human Rights (UNGPs) to identify, prevent, and mitigate human rights harms in which they are involved, and this does not disappear or relax in times of emergency. Further, while derogations of human rights to address public health emergencies are allowed by international human rights law, they are not always necessary, and must be considered on a case-by-case basis.

Although COVID-19 may be the first truly global pandemic of the modern age, it certainly will not be the last—in fact, experts expect that pandemics will become increasingly common. A failure by companies to address the human rights risks associated with their contribution to disease response could lead them to be involved with widespread human rights violations.

However, while the public health crises of the future may share some features with COVID-19, they may vary in other ways too—such as different dynamics of transmission, severity of the illness, availability of treatment, and the necessary control measures—and it will be important to both take the lessons learned from COVID-19 and be able to apply them in different contexts.

A DECISION-MAKING FRAMEWORK FOR COMPANIES

This paper sets out the key elements of a human rights-based approach to the use of data and technology solutions during public health emergencies in today and tomorrow's digital era, with a focus on the role of business and impacts to privacy. Although we focus specifically on public health emergencies, there may be other contexts where the recommendations in this paper may be helpful.

This paper is structured as follows:

First, we present a framework for business decisions in response to public health emergencies.

Second, we provide context about how data and technology solutions are being used to address public health emergencies and how the right to privacy is impacted. We discuss the challenges and lessons learned from this experience, and touch upon the wide range of potential human rights impacts.

Third, we describe the foundations for a human rights-based approach to technology and data use in public health emergencies. We explore international human rights law and relevant regulations, standards, and principles that inform the framework we present in the second section and examine the nature of public health emergencies.

We then lay out a series of recommendations for businesses.

Finally, we explore how state powers have been used around the world to address COVID-19 and other emergencies through several case studies and conclude with questions for further exploration.

There has been much written about technology and data use in the context of COVID-19, from investigations into privacy invasive apps to broad sets of principles to detailed guidance about data use. This paper does not seek to duplicate those efforts and does not propose a new set of principles or data

governance guidelines. Rather, this paper seeks to unite this wide variety of existing thinking under a human rights-based approach grounded in the UNGPs.

KEY QUESTIONS

This paper focuses on the following key questions in the service of a human rights-based approach for companies on the use of data and tech solutions during and after times of public health emergency.

- **Counterbalancing rights:** Human rights can come into conflict with one another for legitimate reasons, and it is important to deploy rights-based methods when two conflicting rights cannot both be achieved in their entirety. Rather than "offsetting" one right against another, it is important to pursue the fullest expression of both and identify how potential harms can be addressed. How should key human rights principles (such as legality, legitimacy, necessity, proportionality, and non-discrimination) be applied to the use of technology and data during and after a public health emergency?

- **Understanding and prioritizing vulnerable groups:** How can we ensure that the needs of the most vulnerable are prioritized when establishing new norms, principles, and standards?

- **Government restriction of rights:** Governments may abuse their powers by placing overbroad restrictions on human rights during a public health emergency, or by extending restrictions beyond the lifetime of a public health emergency. What is the responsibility of companies in these situations?

- **Promoting the right to health:** What is the role of companies in taking actions that promote the enjoyment, realization, and fulfillment of the human right to health during times of public health emergency, over and above company responsibilities under the UNGPs? What are the risks and opportunities associated with companies playing this role?

- **Data for public good:** Innovations in the use of data for public health benefit are happening very rapidly during COVID-19, from epidemiology to public service delivery planning. Are new norms, principles, and standards relating to the use of data for public health benefit emerging that have value beyond the life of the pandemic? Might different norms apply to different types of data?

2. A Human Rights Framework for Business Decisions in Response to Public Health Emergencies

The company responsibility to respect human rights does not disappear during a public health emergency—indeed, the severity of adverse human rights impacts makes it even more essential that companies undertake robust human rights due diligence.

This implies assessing potential adverse human rights impacts and putting in measures to address them in efforts to tackle the public health emergency; for example when developing contact tracing apps in partnership with a government. As companies conduct due diligence, they should include meaningful consultation with stakeholders and preemptive steps to plan for remedy in line with the UNGPs.

The following framework is intended to be used as part of human rights due diligence and guide business decisions related to technology and data use in response to public health emergencies. It is informed by the various elements of international human rights law and relevant regulations, standards, and principles examined later in this paper.

This framework is not intended to provide all the answers or be a box checking exercise. Rather, the framework contains questions to help companies work through key dilemmas and decision points while undertaking human rights due diligence. It should guide companies to make go-no go decisions, structure partnerships, contracts, and agreements in ways that mitigate human rights risk, and to decide when to terminate a contract or stop providing a product or service.

The framework has two parts: before a business decision, and after a contract is signed.

Part One: Before the Business Decision
The first part of the framework encompasses the decision to share or receive data from a government or offer certain products or services in response to a public health emergency. This could be done proactively or in response to a government request.

The framework lists questions the company should answer to determine:

- Whether or not they should pursue the deal.
- How the deal should be structured.
- What mitigations could be put in place.

Part Two: After the Contract
The second part of the framework covers what should be done by the company after a decision is made to provide data or technology solutions to address a public health emergency.

Specifically, the company should:

- Monitor for misuse and abuse.
- Regularly determine whether the product / service / data sharing arrangement is still necessary.

PART ONE: BEFORE THE BUSINESS DECISION

Voluntary vs. Mandatory

Is the company being legally compelled or forced to comply with the request? If so, refer to the Global Network Initiative (GNI) Principles for guidance.

The GNI Principles establish a framework and provide direction for how companies should address government demands, laws, or regulations that do not adhere to internationally recognized human rights standards.

Limitations on rights

- » Does the activity involve limiting non-derogable rights? If yes, do not proceed.
- » Does the activity require limiting rights, or can a fully rights-respecting approach be taken? (i.e., a maximum privacy-preserving approach that still fulfills public health needs)
- » If restrictions are necessary, are they allowed under the ICCPR, ICESCR, or do they require derogation of rights based on emergency powers?
- » If there are rights derogations based on emergency powers, has the government declared state of emergency and advised the appropriate international or regional human rights authority?

Non-derogable rights such as the right to life or freedom of thought cannot be limited or restricted under any circumstances, including states of emergencies.

Rights should not be restricted, even during public health emergencies, unless necessary.

Companies should seek to balance the right to privacy and public health by pursuing the most rights-respecting approach possible to achieving the needed public health goals.

If rights restrictions are needed to achieve the public health goal, companies should consider whether the rights can be restricted based on normal limitations in the ICCPR, ICESCR, or whether they require emergency powers.

If the rights restrictions require emergency powers, a state of emergency needs to have been justifiably declared and the government needs to have notified the relevant human rights bodies.

Human rights principles

Are human rights restrictions:

- » **Provided for by law?** Restrictions must be contained in a national law that is in force at the time the restriction is applied. The law may not be arbitrary or unreasonable and must be clear and accessible to the public—i.e., the type of data collected and how it is shared must be enabled by law.
- » **Necessary?** Restrictions must be necessary for the protection of public health and must respond to a pressing social need. WHO guidance should be considered to establish necessity—i.e., the new form of data collection must be necessary to help public health officials respond.

» **Based on science?** Restrictions to address public health emergencies must be based on science and specifically aimed at preventing disease or injury or providing care for the sick or injured—i.e., the technology solution must address a known component of public health, such as X symptoms are indicative of Y disease.

» **Proportionate?** Restrictions must be proportionate to the interest at stake, and appropriate to achieve the desired public health objective. They must also be the least intrusive option available to achieve the desired result—i.e., the technology solution should not collect real-time geolocation of all users unless absolutely necessary.

» **Non-discriminatory?** Restrictions may not be applied in an arbitrary or discriminatory manner—i.e., the technology solution cannot only be required for members of a certain group.

According to the Siracusa Principles, each of these requirements must be met for rights to be restricted, whether they be restrictions generally allowed by the ICCPR, ICESCR, or restrictions based on emergency powers.
Businesses should ensure any initiative they pursue meets these requirements.

Health and science

Is the activity consistent with the following core obligations of the rights to health and science?

» **Availability:** Will it be widely available to all segments of the population?

» **Accessibility:** Will it be physically, financially, and culturally accessible to everyone without discrimination, in both urban and rural areas, in majority and minority languages?

» **Acceptability:** Will it be culturally respectful? Will it be explained in ways that facilitates acceptance in different cultural and social contexts?

» **Quality:** Is it based on the most advanced, up-to-date, and generally accepted science currently available? Will it be effective?

The ICESCR, which includes the rights to health and science, does not allow for the derogation of rights in any situation. This means that the core obligations of the rights to health and science must be upheld even in times of emergency. Therefore, companies should ensure any initiatives they pursue are consistent with these core obligations.
Note that these core obligations apply principally to "front-end" tech solutions—i.e., public facing solutions that are meant to be used by a large swath of the public. They are less applicable to "back-end" solutions and data sharing arrangements.

Data protection

Does the activity comply with relevant privacy and general data or health data regulations? (e.g. the General Data Protection Regulation (GDPR) in the European Union and the Health Insurance Portability and Accountability Act (HIPAA) in the USA)

Most countries will have privacy or data protection regulations that apply to the proposed tech solution or data sharing arrangement.

These regulations may still apply even in times of emergency, and thus companies should ensure they will be in compliance.

Data use

Will the activity follow other best practices for technology and data use in a public health emergency?

- **Transparency:** The nature of the data collection and/or function of the tool should be clearly explained. The nature of the collaboration with the government must be transparent.
- **Time-bound:** The activity should only continue as long as necessary to address the public health emergency. Personal data should be deleted after it is no longer necessary.
- **Consent:** Personal data should not be collected or shared without securing meaningful consent.
- **Voluntary:** Use of a tech solution or provision of personal data must be voluntary.
- **Data minimization:** Data collected through the technology solution should only be used to respond to the public health crisis. Only the data needed for the response should be collected and retained.
- **Access limitation:** Access to personal data should be limited to those who need the information to conduct treatment, research, and otherwise respond to the public health crisis.
- **Fairness:** Technology tools or data collection should not adversely affect vulnerable populations, and vulnerable groups should be actively considered as part of the design process.
- **Safeguarded from commercial interest:** Companies should not monetize data derived from the use of products or services that help respond to a public health crisis.
- **Accountability:** Companies should take measures to protect against abuse of a technology solution and improper access to personal data.
- **Stakeholder participation:** Design of a tech solution should consider the perspectives of relevant stakeholders, such as public health measures and targeted communities.

- **Efficacy:** There should be evidence that the technology solution will be effective. Models must be reliable, verified, and validated. Tech solutions should be evaluated over time to prove their effectiveness.

- **Non-punitive:** The technology solution or data collection should not be used for any punitive purpose.

These principles come from a variety of entities, including human rights groups, privacy advocates, bioethicists, and companies who have released principles about responsible data and technology use in response to COVID-19. They are grounded in international human rights law and build upon privacy and data protection norms and best practices.

Contracting

Can the contract include prohibited uses to enable the company to challenge misuse / abuse and terminate the agreement if necessary? (e.g. prohibiting the use of data by certain government agencies)

Principle 19 of the UNGPs states that companies should exercise leverage in order to prevent and mitigate human rights impacts. The contractual process is an important point of leverage for companies to prevent and mitigate adverse human rights impacts when they provide tech solutions or data to address a public health emergency. Authorized Use Policies, Privacy Policies, and other contractual terms enable companies to challenge misuse or abuse by a government and terminate the agreement if necessary.

PART TWO: AFTER THE CONTRACT

If the company discovers a government entity is misusing or abusing their business relationship, it can pursue the following options, which are not mutually exclusive:

- Engage with the government entity to request that they cease the behavior.

- Report the concerns to the WHO in order to attempt to address the concerns via diplomatic channels.

- Report the concerns to civil society and/or the media, who can raise alarm and exert public pressure on the offending government.

- If all else fails, terminate the agreement/contract.

The UNGPs expect companies to prevent and mitigate the adverse human rights impacts in which they are involved. This means that even after a contract is signed, companies should review whether their business relationship with a government is resulting in human rights harm.

Principle 19 of the UNGPs states that when the company lacks the leverage to prevent or mitigate adverse human rights impacts, it should consider ending the business relationship, but it should also take into account additional adverse human rights impacts that could result. In the case of tech solutions or data-sharing arrangements to address public health emergencies, which may be key parts of a national pandemic response, terminating a business

relationship could cause significant human rights harm—companies should take this into account before deciding to end a relationship.

Examine whether the product, service, or data-sharing arrangement is still necessary at regular intervals.

If the arrangement involves rights derogations, it should be terminated after it is no longer necessary and the state of emergency has come to an end.

- There is no hard and fast rule for assessing when the public health emergency is no longer an emergency. Companies should first seek to rely on national/regional/local public health authorities.
- In cases where public health authorities may not be reliable or companies suspect that government authorities may be overreaching, they should consult with the WHO and independent health experts like epidemiologists.

If the product/service/data-sharing arrangement does not involve rights derogations, explore whether maintaining or adapting it might be helpful for ongoing public health needs.

International human rights law states that governments should always seek to return to a state of normalcy and that rights derogations in states of emergency must have time limits.

However, in cases where a technology solution or data-sharing arrangement does not involve the derogation of rights, companies may have an opportunity to contribute to public health improvement by maintaining or adapting the initiative. This can be particularly valuable for countries that lack the resources outside of emergencies.

In certain specific instances, there may be opportunities to use the data collected for public health goals outside of the original use case for which data were collected. In these instances, data should not automatically be used for the secondary use cases—instead, the business should first undertake human rights due diligence on the secondary use case and apply privacy best practices.

3. Data Use and Privacy in Global Health Emergencies

To further explore how a human rights framework can inform technology and data use in public health emergencies, it is important to understand how data and technology solutions are used in global health emergencies and how the right to privacy is impacted.

The use of data has long been central to responding to global health emergencies, such as epidemics and pandemics. Health authorities need information such as positive test results, symptom lists, demographic impacts, and movement patterns to understand how diseases spread and effectively mobilize a response.

Personal health information is particularly sensitive and typically subject to stringent national privacy and data protection regulations. The use of this data for public health purposes—to monitor and improve the health of populations—is typically not legally subject to consent, and there is generally strong public support for using data for public health purposes. However, COVID-19's global scale has led to a number of novel technology and data-based solutions to track and combat disease. Many of these solutions also use non-traditional health data and consumer-generated health data, which generally do not receive the same level of privacy protections as traditional health information. This panorama has presented new challenges for striking the right balance between protecting the right to privacy and the right to health.

The digital tools that have emerged in response to COVID-19 each involve a large amount of data collection and often combine various types of data in novel ways. This includes traditional health data, such as symptoms and test results, and other kinds of data, like geolocation and credit card purchasing information. A summary of this can be found in the table on page 17.

The privacy approaches of these tools vary considerably, with some collecting minimal amounts of data and taking a maximum privacy-preserving approach and others collecting large amounts of sensitive information in real time. Here are some examples of digital tools that have emerged or that are being considered in response to COVID-19.

- **Contact tracing and proximity tracking apps** may collect geolocation data, an anonymized, constantly changing ID over Bluetooth, or they may rely on data collected as people interact with other parts of a national data infrastructure. For example, South Korea collects telecommunications data and credit card information.

- **Symptom-tracking apps** ask users to submit details of their symptoms and sometimes other data, such as name, geographical location, GPS location, IP address, social media credentials, age, gender, occupation, medical history, household information, etc.

- **Immunity certificates**, which are being considered as a solution to allow the movement of people during the pandemic, rely on health status data such as antibody test results as well geolocation data or other sensitive data that might be useful to determine someone's risk profile.

- **Quarantine enforcement apps** use geolocation data and sometimes selfies to allow government authorities to monitor a person's location.

» **Flow-modeling tools** use aggregated, anonymized sets of geolocation data to provide insights into the effectiveness of public health policies. For example, Google's COVID-19 Community Mobility Reports show movement trends over time by geography and across different categories of places, such as retail and residential.

However, these tools are only the public-facing **"front end"** of technology and data use for public health response. Behind each of these tools, coordinating and informing the larger government-led public health response, is a **"back end"** of systems that are largely out of public view. These "back end" systems control how data flows and how it is used by enabling data sharing between and across government agencies, and they often combine different datasets for analysis.

For example, in the United Kingdom, the National Health Service's (NHS) "COVID-19 Data Store" combines datasets from a wide variety of sources to enable near real-time public health surveillance, and the NHS's OpenSAFELY analytics platform enables data analysis across over 24 million pseudonymized patient primary care records. While the "front end" systems have received more media coverage and public scrutiny, much less is known about the "back end" tools. These systems tend to aggregate data from multiple sources and can have a significant impact on the right to privacy. However, the widespread lack of transparency has prevented even dedicated researchers from discovering the opportunities and risks of these systems.

Although we expect government entities to lead public health responses, the private sector is necessarily involved, whether they are part of the health system (e.g. private hospitals, pharmaceutical companies, and insurance companies), provide infrastructure and services to public health authorities that are useful for disease response (e.g. cloud solutions used for data aggregation, management and analysis, or operating systems for apps), or because they have data that is useful for disease response (e.g. technology companies with geolocation data or social network data that can help understand transmission dynamics and monitor compliance with government mandates).

The table below shows the different ways in which the private sector has been involved with the collection and use of data during COVID-19 as well as some of the risks associated with different types of data.

Types of Data and Data Use Cases during COVID-19				
Type of Data	**Examples**	**Use Cases**	**Business Involvement**	**Risks**
Traditional health data	Diagnoses, test results, medical claims, rate of infection, characteristics of the virus, etc.	Medical care, disease surveillance, R&D, immunity certification, return to work efforts	Private healthcare providers, pharmaceutical companies, insurance companies, tech providers	Unnecessary or disproportionate mass data collection. Poor data management and security practices. Lack of anonymization or risk of re identification Unnecessary and/or unregulated data sharing between entities Non-consensual disclosure of personal data. Combining different types of data to reveal private information. Lack of regulatory protections for non-traditional health data and consumer health data. Illegitimate surveillance of a population
Consumer-generated health data	Data collected through smart health devices, wearable tech health apps, web searches etc.	Symptom tracking, medical care	Health apps or wearable devices that collect this type of data are owned by companies.	
Non-traditional health data	Cell tower data, Call Detail Records, IP data, geolocation data, proximity data, social network data, financial transaction data etc.	Contact tracing, proximity tracing, quarantine enforcement, flow modeling	Businesses collect this data as part of their services and are asked to share it with the government.	

THE FORESEEABLE CHALLENGES OF TECH SOLUTIONS FOR PUBLIC HEALTH EMERGENCIES

Although the pandemic is far from over, the use of novel technology to address COVID-19 has already generated challenges, mistakes, and lessons learned. As governments and companies around the world rushed to implement technology-based solutions, they encountered numerous challenges and succumbed to pitfalls and practices that have been documented by both the humanitarian data and the technology for development sectors for some time. Understanding these challenges and their interconnectedness will be important for addressing the potential adverse human rights impacts arising from data and technology-based solutions to public health emergencies.

- **Tech-solutionism:** Leaders are often drawn to "easy" technology-based fixes as a solution to complex problems. However, technology solutions are rarely the panacea. In a world with uneven access to technology and the internet and varying digital literacy rates, technology-based solutions can never be a silver bullet. Human involvement is always a necessary component—for example, contact-tracing apps are most effective as aids to human contact-tracing efforts.

- **Trust and uptake matter:** In countries where people distrust their government or are wary of health data collection, voluntary technology-based tools suffer from low levels of uptake, which drastically decreases their effectiveness.

- **Lack of evidence of effectiveness:** In some cases, technology solutions have been used without a clear understanding of whether they will be effective. One example is thermal imaging cameras, which are designed to take the temperatures of people in the vicinity—but not everyone with COVID-19 will have a high fever, and people often get fevers for other reasons unrelated to COVID-19. Thermal cameras miss infected people with other symptoms or no symptoms, and they will also falsely flag people with fevers for another reason.

- **Lack of evidence about what data collection is necessary for effective public health responses:** Although narrowly scoped tools and maximum privacy-based approaches preserve the privacy rights of individuals and prevent scope creep, some public health experts argue that they can undermine disease response. Because many of the digital tools used for COVID-19 response are new, there is a lack of evidence about what level of data collection is needed for the tools to be effective. This makes it challenging to take a science-based approach to identifying the appropriate amount of data collection needed without unduly infringing on privacy.

- **Blurred lines and regulatory gaps between traditional health data and consumer health data:** The digitization of life has resulted in massive volumes of non-traditional health data that can be useful for public health responses, such as movement patterns, credit card transactions, and consumer-generated health data from things like fitness trackers. However, despite these types of data being used for public health purposes, they are typically not regulated as strictly as traditional health data, allowing for blurred lines and loopholes that can enable mass privacy infringement.

- **Lack of transparency:** Although public-facing "front end" tools have received more scrutiny than "back end" systems, technology solutions for COVID have lacked transparency—for example, it is often unclear how data is shared between governments and companies and across government

departments. The contracting process is also often both opaque and rushed, with companies receiving contracts without competition terms or beginning work without any contract at all.

» **The control of digital infrastructure by a few companies:** Digital infrastructure, including cloud platforms and operating systems, are central to any technology solution that is used to respond to the pandemic. Today, this infrastructure is privately owned and operated by a few companies, giving these entities disproportionate control over the design and use of technology solutions, such as the infrastructure that makes contact tracing apps work. Similarly, digital information infrastructure and delivery platforms are controlled by private sector companies without sufficient oversight and regulation. The control of digital infrastructure by a few companies, and the lack of access to this infrastructure by governments, can be problematic considering the critical role these platforms play as public utilities during public health emergencies.

» **Disparate geographic impacts and the digital divide:** Data and technology-based solutions rely on people having access to technology and the know-how to use it as well as the existence of sufficient data. In general, technology-based solutions tend to help the most well off and exclude the least well off—in places with disconnected communities and data-poor environments, COVID-19 solutions have already exacerbated the digital divide.[2]

» **Low government technology literacy and management capacity:** Many governments lack the knowledge and resources to properly design and manage technology-based pandemic response solutions at scale. This has resulted in many bungled government-led technology efforts, such as contact-tracing apps that revealed real-time GPS location data to numerous entities and the leak of personal records from symptom trackers.

[2] An example of this can be found in India, where the government-mandated contact-tracing app was initially inaccessible to the majority of the population, which does not have access to a smartphone, https://www.wired.co.uk/article/india-contact-tracing-app-mandatory-arogya-setu. Later, the government made a similar version of the app available to people with landline phones, https://swachhindia.ndtv.com/fight-against-covid-19-aarogya-setu-app-now-accessible-to-people-without-smartphones-44984

OTHER HUMAN RIGHTS IMPACTS

Although privacy may be the human right most impacted by business involvement in public health emergency responses, it is far from the only one. Human rights are interrelated and interdependent, and it is rare for a single right to be impacted in isolation. Although this paper primarily focuses on the right to privacy, it is important to acknowledge the other key human impacts of tech and data use for public health emergency response, including:

- **Equality and Non-Discrimination:** Technology solutions may be less readily available to those who lack access to healthcare and smart phones or those who are undocumented. These rightsholders are disproportionately women; racial, ethnic, and national minorities; older persons; and other vulnerable groups. In countries characterized by surveillance, poor rule of law, or a history of systematic discrimination, rightsholders such as racial minorities, human rights defenders, and political activists may be reluctant to enroll in government-run programs.

- **Freedom of Movement and Freedom of Association and Assembly:** Tech-based COVID-19 solutions such as quarantine enforcement apps may be used to restrict movement, assembly, and association beyond that which is necessary and proportionate. Vulnerable groups with less access to testing or vaccination could have their rights disproportionately restricted. The use of technology products to control access to mass transit, public spaces, and public buildings are particularly relevant.

- **Health:** By helping to enable beneficial public health outcomes and targeted health interventions, technology solutions can have a positive impact on the right to health. However, some products, such as immunity certificates, could incentivize people to become infected, adversely impacting the health and wellbeing of themselves and others.

- **Right to Work and to Just and Favorable Conditions of Work:** Technology solutions used to monitor employee health status and facilitate employer data collection could improve the right to work and access to employment opportunities, especially for those unable to work from home or in need of regular income. However, these tools come with significant privacy trade-offs, and vulnerable groups with less access to testing or vaccination could have their right to work disproportionately restricted.

- **Right to enjoy the benefits of scientific progress:** Public dialogue places emphasis on restrictions to freedom of movement, yet the most vulnerable (e.g. essential workers) do not face the same restrictions. Similarly, public dialogue emphasizes privacy violations, yet the most vulnerable (e.g. undocumented migrants, low income populations) don't have the same volume of data to share. How can we ensure that the needs of the most vulnerable are prioritized when establishing new norms, principles, and standards?

- **Vulnerable Groups:** Vulnerable groups are disproportionately impacted by adverse human rights impacts in public health emergencies. This is partially due to the social determinants of health--marginalized groups often have less access to food, clean water, sanitation, education, and medical care and are therefore most impacted by disease. It is also closely related to the digital divide that prevents vulnerable communities from reaping the benefits of tech solutions.

4. Foundations for a Human Rights-Based Approach

Governments have obligations under international human rights law to respect, protect and fulfill human rights and hold primary responsibility to respond to health emergencies. International human rights law also gives states the legal possibility to limit the enjoyment of certain rights during an emergency, subject to certain procedures and boundaries. We know from both past emergencies and COVID-19 examples in a variety of countries—such as Hungary, Russia, India, the U.S., and the UK—that governments often overreach in ways that unduly restrict rights.

While governments have a duty to protect human rights, companies have a responsibility to respect human rights as outlined in the UNGPs, irrespective of whether governments meet their obligations set out in international human rights law. The responsibility to respect human rights applies during a public health emergency, and it implies undertaking human rights due diligence in any efforts to respond to or address the public health emergency, e.g. when developing contact tracing apps in partnership with a government. This includes identifying risks of government overreach beyond what they can legally do in accordance with their human rights obligations.

There is no provision for the derogation of the business responsibility to respect human rights in the same way that states can derogate certain rights under human rights treaties. However, it is important for companies, when engaging with governments and devising their own responses to a public health emergency, to consider the human rights implications of derogated rights and mitigating the impact of their own role in such a context.

To achieve this, companies should draw upon a framework—such as the one presented in the second section of this paper—that is based on international human rights law and outlines how governments can declare states of emergency and legitimately derogate rights, as well as the obligations of states to protect the rights to health and science. Our framework draws upon:

- Article 4 of the International Covenant on Civil and Political Rights (ICCPR)
- The Siracusa Principles on the Limitation and Derogation Provisions in the ICCPR
- The Committee on Economic, Social and Cultural Rights' General Comment 14 on the Right to Health and General Comment 25 on the Right to Science

While these texts form a foundation for determining appropriate government and company actions related to public health emergencies, they are high level and difficult for companies to operationalize and apply to specific decisions, such as whether to provide certain data or services to a government entity or whether to develop a certain tech tool. Therefore, our framework is also informed by other regulations and norms for more specific guidance, such as:

- Existing privacy legislation, including general data protection regulations, such as the GDPR, and health regulations, such as the HIPAA.
- Guidance and principles, including:
    - The Global Network Initiative (GNI) Principles
    - Humanitarian data standards

- Bioethics principles
- Civil society and company principles related to data use and COVID-19

Here we examine in more detail the international human rights law and associated principles that inform the human rights framework presented in the second section of this paper.

STATES OF EMERGENCY AND DEROGATIONS OF RIGHTS

The first element to a human rights framework for business decision-making in public health emergencies is understanding how derogations of rights are allowed during states of emergency.

International human rights law recognizes that sometimes governments may need to restrict the rights of their citizens for legitimate aims, both in normal times and to respond to a national emergency—however, the ability of governments to restrict rights is not unbounded**.** The ways in which governments may legitimately limit rights is laid out in Article 4 of the ICCPR, various other articles pertaining to specific rights, and the Siracusa Principles.

Some rights in the ICCPR can be limited without a state of emergency. These include freedom of movement (Article 12), Freedom of Expression and Opinion (Article 19), and Freedom of Assembly and Association (Articles 21 and 22). These rights can be subject to restrictions provided for by law and necessary for "respect of the rights of others" and "for the protection of national security, public order, or public health or morals."

Furthermore, Article 4 of the ICCPR allows states to derogate rights in times of public emergency. A public emergency is defined as “an exceptional situation of crisis or public danger, actual or imminent, which affects the whole population or the whole population of the area to which the declaration applies and constitutes a threat to the organized life of the community of which the state is composed.” States that invoke Article 4 must issue a formal declaration of emergency and notify the UN with sufficient justification for the derogations.

According to the Siracusa Principles, a state of emergency may be justified for public health reasons if a state must deal with a serious threat to the health of the population. It is expected that emergency powers be **time-bound and temporary** and that states should **aim to return to a state of normalcy as soon as possible.**

OHCHR Guidance on COVID-19 States of Emergency:

- States should attempt proportionate restrictions on allowable rights prior to invoking Article 4 states of emergency.
- Emergency measures should be strictly temporary and the least intrusive needed to achieve public health goals, and they should include safeguards such as sunset or review clauses to ensure a return to normal as soon as the emergency is over.
- States of emergency should be guided by human rights principles, including transparency.
- States of emergency should not be used for any other purpose than what it was declared for. It should not be used to stifle dissent.

Importantly, **a few rights are considered "non-derogable,"** meaning they **cannot be restricted even in a state of emergency.** These include the right to life, freedom from torture or inhuman and degrading treatment (including from medical or scientific experimentation without consent), freedom from slavery, imprisonment for failing to fulfill a contractual obligation, retroactive criminal punishment, right to recognition as a person before the law, and freedom of thought, conscience, and religion.[3]

The International Covenant on Economic, Social, and Cultural Rights (ICESCR) includes no provisions for derogations. However, Article 4 recognizes that states "may subject such rights only to such limitations as are determined by law only in so far as this may be compatible with the nature of these rights and solely for the purpose of promoting the general welfare in a democratic society." That said, even in states of emergency, governments must still comply with the core obligations of the rights to food, health, housing, social protection, water and sanitation, education, and an adequate standard of living.

According to the Siracusa Principles and guidance released by the OHCHR specific to emergency measures and COVID-19, any limitation on rights, whether they be via Article 4 of the ICCPR or as part of the specific limitations enabled by the ICCPR, must adhere to the following principles:

- **Legality:** The restriction must be "provided for by law." This means that the limitation must be contained in a national law that is in force at the time the limitation is applied. The law must not be arbitrary or unreasonable, and it must be clear and accessible to the public.

- **Necessity:** The restriction must be necessary for the protection of one of the permissible grounds stated in the ICCPR, which include public health, and must respond to a pressing social need. Restrictions to address public health emergencies must be based on scientific evidence and specifically aimed at preventing disease or injury or providing care for the sick or injured. States should look to WHO guidelines to establish necessity.

- **Proportionality**: The restriction must be proportionate to the interest at stake, i.e. it must be appropriate to achieve the desired objective, and it must be the least intrusive option among those that might achieve the desired result.

- **Non-discrimination**: Restrictions may not be applied in an arbitrary or discriminatory manner.

THE RIGHT TO HEALTH AND THE RIGHT TO SCIENCE

The rights to health and science are two interrelated rights enumerated in the ICESCR that are particularly relevant to public health emergencies—they are the positive rights impacts that we are ultimately seeking to achieve. Enabling the responsible use of data and tech solutions during public health emergencies is important to realizing these rights. However, the rights to health and science are too often underexplored in the technology and human rights field.

In the case of COVID-19, many states are restricting other rights in order to protect the right to health, and they are using science in the form of vaccine and pharmaceutical research and technology to protect the right to health as well. Although it may seem that the rights to health and science would inherently be protected during public health emergencies, this is not necessarily the case. For example, both

[3] Additionally, there are other rights not listed in the ICCPR as non-derogable but can be considered non-derogable according to international human rights law norms. This includes prohibitions on taking hostages, imposing collecting punishments, and arbitrary deprivation of liberty, right to a fair trial, fair treatment of prisoners, deportation without grounds permitted under international law, and forced displacement.

government and citizen-generated COVID-19 misinformation has had adverse impacts on both the right to health and the right to science.

The ICESCR contains no provisions for derogations, so states are still required to uphold their core obligations for the right to health and the right to science during times of emergency. This means that **during public health emergencies, state measures designed to protect public health and the pursuit of scientific advancement to address the health crisis, as well as the related activities of companies, should be in line with the core obligations of the rights to health and science.**

The core obligations for both the right to health and science are known as the "Triple A-Q" framework, consisting of availability, accessibility, acceptability, and quality. These are enumerated in General Comment 14 on the Right to Health and General Comment 25 on the Right to Science and are listed in the table below.[4]

Core Obligations of the Rights to Health and Science		
	Right to Health	**Right to Science**
Definition of the Right	» Freedom to control one's health and body » Right to a system of health protection that gives everyone equal opportunity to enjoy highest attainable level of health » Providing for the underlying determinants of health: potable water, sanitation, food, housing, environment, health education » Participation of the population in health-related decision-making » Includes the right to prevention, treatment, and control of diseases	» Stems from the capacity of science to improve the well-being of humankind » Includes both natural and social sciences, and refers to both the process and the results » Includes the technology that is a product of scientific advancement » "Benefits" include vaccinations and medication
Core Obligation 1: Availability	» Sufficient quantity of health care services and facilities available to all segments of the population	» Availability of services that ensure access to scientific knowledge to everyone, including internet networks, libraries, etc.
Core Obligation 2: Accessibility	» Health goods and services must be accessible to everyone without discrimination. » Particular emphasis on access for vulnerable groups » Includes access to underlying determinants of health, affordability, and information[5]	» Services must be physically, financially and culturally accessible without discrimination, in both urban and rural areas, in majority and minority languages, for all groups and persons.
Core Obligation 3: Acceptability	» Health services and facilities must be culturally respectful	» Ensuring results of research and scientific progress are explained and disseminated to facilitate their acceptance in different cultural and social contexts.

[4] Table sources: General Comment 25 on the Right to Science, https://undocs.org/E/C.12/GC/25; General Comment 14 on the Right to Health, https://digitallibrary.un.org/record/425041?ln=en.
[5] Access to technology and digital skills may also be considered a social determinant of health. See https://www.goodthingsfoundation.org/sites/default/files/research-publications/digital_inclusion_in_health_and_care-_lessons_learned_from_the_nhs_widening_digital_participation_programme_2017-2020__0.pdf.

		» Scientific advancements should be tailored to needs of special populations, such as persons with disabilities.
Core Obligation 4: Quality	» Health services must be scientifically and medically appropriate and of good quality	» Scientific creation and applications should be based on the most advanced, up-to-date, and generally accepted science available at the time.

LIMITATIONS OF INTERNATIONAL HUMAN RIGHTS LAW

Although International Human Rights Law provides general guidance and establishes some clear redlines related to states' ability to restrict human rights, it is **difficult to operationalize in the context of a public health emergency**. As health and human rights scholar Nina Sun argues in "Applying Siracusa: A Call for a General Comment on Public Health Emergencies," the Siracusa Principles do not account for the complexities of public health crises.

There are three reasons she provides for this challenge.

First, public health crises are diverse. For example, there can be different dynamics of transmission, the severity of the illness can vary, treatment may or may not exist, and the necessary control measures may differ. Second, there is significant uncertainty during outbreaks of new diseases since the science develops in real time, and this makes it difficult to assess whether responses are evidence-based or arbitrary. And third, the impact of a pandemic depends heavily on national and even local context—it ebbs and flows in different places at different times and impacts different places in different ways.

Given this context, Sun calls for an ICCPR general comment on derogations from and limitations on human rights for public health reasons that provides specific guidance to address the necessity and proportionality of state responses and the misuse of emergency powers.

In addition, because international human rights law relating to permissible restrictions of human rights and states of emergency is geared toward states and applies to the range of reasons for restrictions and states of emergency, as well as the entire range of human rights, it is necessarily high level. This can make it difficult to operationalize what otherwise seem like clear principles to apply to the nuances of a given policy or business decision, particularly for issues as complex as privacy and data use.

INTERNATIONAL REGULATIONS, STANDARDS, AND PRINCIPLES

To fill the gaps in international human rights law and create an operationalizable framework for companies to make business decisions related to technology and data use in public health emergencies, we also looked at relevant international regulations, standards, and principles.

These include:

- Regulations on data privacy including general data protection regulations, such as the GDPR, and health data regulations, such as the HIPAA.

- Guidance and principles for tech and data use in public health emergencies by civil society, private sector companies, and bioethicists.

1. How the GDPR Addresses Privacy and Data Protection Rights Restrictions

The E.U.'s General Data Protection Regulation (GDPR) is generally considered to allow most of the data processing needs that arise in public health emergencies.

Article 23 of the GDPR allows member states to restrict certain rights of the data subject to safeguard public interest, including public health. Restrictions of rights must respect the essence of the right being restricted, be provided for by law, be purpose limited, necessary and proportionate.

Recital 46 recognizes as lawful the processing of personal data for the public interest and specifically refers to "monitoring epidemics and their spread" as one such lawful use. Provisions in Article 6 and 9 allow for collection, use, and sharing of personal data related to health in the context of an epidemic, without the need for explicit consent of the data subject.

In its guidance on restrictions related to COVID-19, the European Data Protection Board made clear that "the GDPR remains applicable and allows for an efficient response to the pandemic, while at the same time protecting fundamental rights and freedoms." The board also stated that the GDPR "enables data processing operations necessary to contribute to the fight against the spread of a pandemic." It follows that suspension of data protection rights by countries, such as Hungary, is not necessary.

Data Protection Authorities, who oversee ensuring compliance with the GDPR in each E.U. member state, have traditionally played a supervisory and enforcement role related to government data collection. However, in the context of COVID-19, some have chosen to also act as an advisor to the government as well. This has required them to operate outside of their core competency of personal data and means there are regulatory gaps related to the use of non-personal data during public health crises.

2. How Health Data Regulations Address Restrictions

Health data generally refers to any data about a person collected in a medical setting. This includes elements such as medical history, demographic information, diagnoses, test or lab results, vaccine records, and mental health conditions. Health data is universally considered particularly sensitive, and thus is generally subject to specific privacy and data protection requirements. This is typically governed by national law, and as a result the health data protection space is quite fragmented.

The closest thing to international health data regulations is the WHO's International Health Regulations, which apply to all WHO member states. In the context of data use and public health emergencies, Article 45 on the Treatment of Personal Data allows state parties to "disclose and process personal data where essential for the purposes of assessing and managing a public health risk." However, it ultimately defers to national law.

One prominent national health data regulation is HIPAA (Health Insurance Portability and Accountability Act) in the United States. Its section on Disclosures for Public Health Activities allows "covered entities to disclose protected health information without authorization for specified public health purposes." To address COVID-19, new waivers enabled businesses to disclose health information related to public health and health oversight activities. However, HIPAA does not protect health information collected outside a healthcare facility. This means, for example, that COVID-19 testing done by a private company is not protected under HIPAA.

In addition to the issues of fragmentation, **health data protection regulations have some important limitations,** and **other kinds of data are increasingly combined with traditional health data and used for health purposes.**

For example, consumer-generated health data typically collected by fitness trackers and wellness apps are not always subject to privacy and data protection requirements—yet in the case of COVID-19, this kind of data could include anything from temperature scanning apps to web searches on COVID-19 symptoms. Due to the lack of protections for this type of unregulated health data, the sector relies on best practices. Some examples include the CARIN Code, which lays out opt-in/opt-out strategies for mobile health data, the Center for Democracy and Technology's new framework for unregulated health data, and the Future of Privacy Forum's best practices for consumer generated genetic data. Increasingly, advocacy organizations are calling for the redefinition of health data to include any data that is being used for health purposes, regardless of its source.

3. Principles for Digital Surveillance and Data Use During COVID

In response to the wave of new technologies and uses of data to address COVID-19, and the associated privacy and surveillance concerns, **entities from civil society and the private sector have published principles for technology and data use that go far beyond the lawful, necessary, and proportionate requirements set out by the international human rights treaties**. These principles typically build upon existing global privacy norms and best practices, such as those codified in the GDPR.

In addition, the humanitarian data community's evolving development of norms for data use in humanitarian emergency response also apply to public health emergencies. Many of these principles and the associated guidelines provide detailed instructions related to data use and management that are highly relevant.

Below we explore the key themes that have emerged from the various principles, standards, and guidelines published by civil society coalitions, companies, bioethics groups, and the humanitarian data field.

Principles for Data Use and Tech for Public Health Emergencies[6]	
Principle	**Description**
Transparency	Any use of data and technology must be clearly and quickly explained to the public. Collaborations between governments, companies and other organizations must be transparent.
Time-Bound	Measures must be in place only for as long as necessary to address the emergency; data must only be retained as long as is necessary for the purposes for which it was collected.
Purpose Limitation, Data Minimization	Data collected must only be used for the purposes of responding to the emergency. Technologies must collect and retain only the data that is essential for a solution to be effective. Public health authorities should provide input regarding the types of data that will be most useful for fighting the pandemic.
Access Limitation	Access to health data should be limited to those who need information to conduct treatment, research, and otherwise address the crisis.
Privacy and Data Protection	Personal data protection must be upheld in all emergency measures.
Data Security	Measures must include protections to secure any collected data.
Non-Discrimination, Fairness	Measures should not adversely affect already vulnerable populations, and the underserved should be actively considered in design process.
Safeguarded from Commercial Interest	Private companies should not be able to monetize data derived from the use of their products that help respond to the public health crisis.
Rights-Respecting	Businesses involved in efforts to tackle COVID-19 must undertake due diligence to ensure they respect human rights.
Accountability, Safeguarded from Abuse, Oversight	Measures must incorporate accountability protections and safeguards against abuse. They must be subject to effective oversight by independent bodies.
Due Process, Access to Remedy	Individuals who have been subjected to undue restrictions of their rights must have access to effective remedies, including the opportunity to timely and fairly challenge these conclusions and limits.
Stakeholder Participation	Measures should include meaningful participation of stakeholders, in particular experts in the public health sector and the most marginalized population groups.
Efficacy / Testing and Evaluation	There must be evidence that measures will be effective prior to deployment and they should be rigorously evaluated over time to prove their effectiveness. Algorithmic models must be reliable, verified, and validated.
Consent / Data Control	An individual's data should not be collected or shared without securing the individual's meaningful consent.
Voluntary	Measures must be voluntary and not mandatory.
Non-Punitive	Measures must not be used for any punitive purpose or legal proceedings.

[6] This table pulls from the following sets of principles:

- WHO Guidance on Contact Tracing Tech
- Joint Civil Society Statement on the Use of Digital Surveillance Tools
- Civil Rights Groups Principles on COVID-19 Tech
- INCLO Surveillance Tech and COVID-19 Principles
- Protecting Civil Liberties During a Public Health Crisis, EFF
- A rapid evidence review on the technical considerations and societal implications of using technology to transition from the COVID-19 crisis, Ada Lovelace
- Recommendations on privacy and data protection in the fight against COVID-19, Access Now
- GSMA COVID-19 Privacy Guidelines
- Microsoft Privacy Principles for COVID-19 Tech Solutions
- Salesforce Privacy and Ethical Use Principles for COVID-19 Response
- Ethical considerations in responding to the COVID-19 pandemic, Nuffield Council on Bioethics
- Guide to the ethics of surveillance and quarantine for novel coronavirus, Nuffield Council on Bioethics
- Data Responsibility in the COVID-19 Response, UN OCHA Centre for Humanitarian Data
- Handbook on data protection in humanitarian action, ICRC
- UN Joint Statement on Data Protection and Privacy in the COVID-19 Response

5. Understanding Public Health Emergencies

In addition to understanding how human rights may or may not be limited during times of public health emergency, it is also important for companies to understand what constitutes a legitimate public health emergency, who decides, and how we know when it is over in the context of a pandemic without a clear universal end point.

Although companies should be able to rely on public health authorities to say when emergency measures are no longer necessary and rights restrictions can sunset, **companies may find themselves forced to make a call** about whether to continue a given activity, offer services, or share data **in the face of a government seeking to illegitimately expand its surveillance powers.**

THE ROLE OF THE WORLD HEALTH ORGANIZATION

The WHO can formally declare international health emergencies, called Public Health Emergencies of International Concern (PHEIC).

A PHEIC is defined in the International Health Regulations (IHR) as "an extraordinary event which is determined to constitute a public health risk to other states through the international spread of disease and to potentially require a coordinated international response." This definition implies a situation that is serious, sudden, unusual, or unexpected; carries implications for public health beyond the affected state's national borders; and may require immediate international action.

The WHO declared that the COVID-19 outbreak constitutes a PHEIC on January 30, 2020.

The IHR Emergency Committee advises the WHO Director-General on recommended measures to address the situation, known as Temporary Recommendations. In the context of COVID-19, the Committee advised state parties to support research efforts, maintain essential health services, and to strengthen public health surveillance for case identification and contact tracing. **Governments were advised to take proportionate measures based on risk assessments and to review measures regularly.**

Temporary Recommendations automatically expire three months after they are issued, then the Emergency Committee reviews the current epidemiological situation at least every three months.

Importantly, the WHO does not have enforcement authority with respect to a PHEIC. Rather, the International Health Regulations are grounded in a state-centric model for disease containment based on voluntary cooperation by countries. The WHO publicly acknowledges that it relies on "peer pressure" and "public knowledge" as the primary incentives for voluntary compliance with international obligations.

STATE OF EMERGENCY DECLARATIONS AND DEROGATIONS

As the first truly global modern pandemic, there are an unprecedented number of human rights derogations taking place during COVID-19.

At the time of writing, more than 10 percent of countries have formally derogated some of their obligations under international human rights law, although only six (Armenia, Ecuador, Estonia, Guatemala, Latvia, and Romania) have notified the UN as is required.

Many countries have also derogated rights under their regional human rights covenants as well—10 countries have derogated from obligations under the European Convention on Human Rights[7] and 15 countries have derogated from the American Convention on Human Rights.[8] Many more countries have declared de-facto states of emergencies without proper notification to the relevant human rights bodies as required under Article 4 of the ICCPR.

Most derogations relate to freedom of movement, assembly, and association. However, other governments have also chosen to derogate the rights to liberty and fair trial, as well as privacy.[9] These derogations have led to suspension of in-person classes at schools, the prohibition of public gatherings, restrictions on visits to hospitals and detention facilities, restrictions on spending leisure time by closing sports clubs, gyms etc., restriction on cross-border movements, and quarantine requirements.

There are different schools of thought on the role and necessity of state of emergency declarations. One argues that because of the risk of countries abusing emergency powers, the best thing to do is to resist panic and insist on the principle of normalcy. This means handling the crisis through normally applicable powers and procedures and not restricting any rights.

The other argument is that officially declaring a state of emergency, and notifying international institutions about measures that derogate from some of their human rights obligations, may actually constrain emergency powers by requiring the state to articulate their emergency measures under the terms of the Siracusa Principles and a commitment to human rights as a framework for legitimate emergency measures.

The context of COVID-19 has led to several important questions about emergency powers and derogations of rights in response to a public health emergency.

The first question is if governments truly need to derogate rights to combat the pandemic. The Council of Europe staked a position on this by stating they “are not actively encouraging or obliging member states to make such notifications,” and are instead encouraging member states to restrict rights as necessary based on existing allowable provisions in the ECHR.

The second question is whether these derogations and the resulting measures help fight the pandemic. Some of the hardest hit countries did not derogate from the ICCPR or the ECHR, and found ways to fight the pandemic within the framework of permissible limitations—for example, Italy passed a decree to create a special legal framework to collect/share health data during the pandemic. Given the risk of

[7] As of August 2020 these included Albania, Armenia, Estonia, Georgia, Latvia, Moldova, North Macedonia and Romania, San Marino, and Serbia.
[8] As of August 2020 these included Argentina, Bolivia, Chile, Colombia, Ecuador, El Salvador, Guatemala, Honduras, Panama, and Peru, the Dominican Republic, Suriname, Paraguay, Venezuela, and Jamaica.
[9] Estonia and Latvia have derogated the rights to liberty and fair trial. Estonia and Romania have derogated privacy.

emergency powers and associated rights restrictions becoming permanent, they should be both necessary and effective to address a public health emergency.

This leads to a key question: What should a company do if it makes a business deal with a government in relation to a public health emergency and there is reason to suspect the government may be using the company's products and services to unduly infringe on people's rights—for example, by using disease surveillance tools for surveillance and repression of an ethnic or religious minority?

The first step would be to engage with the government to try to end the behavior. If that is not successful, the most obvious option is for the company to terminate the deal, assuming its contract with the government entity prohibits that kind of misuse.

Another option is for the company to go directly to the WHO to report their concerns. The WHO can then go through its diplomatic channels to try to address the issue. A final option is for the company to report the problem to civil society actors in that country who can raise the alarm via media attention. In some cases, this option might be more effective than diplomatic channels.

WHO DECIDES WHEN THE EMERGENCY IS OVER?

Beyond the issue of whether a state of emergency is necessary and the rights restrictions pursued to are legitimate is a key question: Who decides when the emergency is over?

International human rights law stipulates that states of emergency must be time bound and rights restrictions should last only as long as necessary. Best practice suggests that **companies should instate sunset clauses or time limits on contracts to ensure that rights limitations they are party to do not last longer than they should.** To do this, however, there needs to be **a clear picture of when the public health emergency is "over"**—or at the very least, when emergency measures are no longer necessary**.**

Unfortunately, defining when a public health emergency is "over" is far from simple. In the case of the COVID-19 pandemic, there will be no universal end date. The pandemic will ebb and flow across and within national borders; some countries may be ready to relax emergency measures while others are still experiencing a high number of cases.

Government authorities are ultimately responsible for declaring an end to a state of emergency. However, the long history of states abusing emergency powers to consolidate power and institutionalize the ability to violate human rights long-term suggests that some states will choose to extend their emergency powers beyond what is scientifically and medically necessary. In this case, companies may find themselves needing to assess whether a government request or contract is legitimate or not, or whether they should continue sharing certain data or providing certain services.

In this instance, companies should regularly review whether the product, service, or data sharing arrangement they have with a government is still necessary. If the activities involve rights restrictions, they should be sunset after they are no longer necessary and the state of emergency is over.

However, there is no clear rule for assessing when the public health emergency is no longer an emergency. Companies should first seek to rely on national, regional, and even local public health authorities—and in cases where public health authorities may not be reliable, or companies suspect

government authorities may be overreaching, they should consult with the WHO and independent health experts.

If the product, service, or data sharing arrangements do not involve rights restrictions, companies should explore whether maintaining or adapting might be helpful for ongoing public health needs. Crises often provide needed resources for innovation, and technology and data use developments could prove beneficial to public health efforts in the long run.

6. Recommendations

In addition to utilizing the human rights framework for business decisions presented in this paper, there are several other strategies companies can deploy in a rights-based approach to the use of technology in public health emergencies. The following recommendations are presented according to BSR's "act, enable, influence" framework to guide company action on all sustainability issues, including human rights.

ACT: WHAT COMPANIES SHOULD DO INTERNALLY

- **Make business decisions in response to public health emergencies using a human-rights based framework.**
  Companies' obligations under the UNGPs to carry out human rights due diligence to identify, prevent, and mitigate their human rights impacts does not disappear during times of emergency. Companies should undertake human rights due diligence to foresee possible impacts of their decisions. This due diligence should include meaningful consultation with stakeholders and preemptive steps to plan for remedy in line with the UNGPs. For company decisions specifically related to technology and data use in the context of public health emergencies, we hope the framework outlined in this paper is useful for companies seeking to balance privacy rights with the protection of public health.

- **Avoid known pitfalls.**
  While it may be tempting to rapidly define how a company's products and services could contribute to addressing a public health crisis, thorough (yet speedy) deliberation is needed to determine the extent a product or service might be effective and whether a data or technology-based solution is the best approach. The following recommendations are intended to help companies avoid known pitfalls related to working with governments during times of emergencies:

  - **Take care to avoid falling into the tech-solutionism trap.**
    Consider how technology can augment necessary involvement by humans rather than be the entire solution—a less "exciting" solution is sometimes more impactful. For example, rather than building a new tool, it might be more impactful for companies to explore how they can support or augment existing efforts.

  - **Review the effectiveness of escalation processes for handling government requests and contracts during times of emergency, and if needed, create a new one.**
    Each case should be examined on its relevant merits to balance the public health need with the risk of government overreach. Internal stakeholders from multiple areas should be involved to ensure a comprehensive examination of the risks and opportunities. The human rights risk will be determined by a combination of the human rights record of the country in question, the nature of the specific entity, and the data use, use case, product, or service. Companies should take special care with dual use technology applications that can also be used for illegitimate surveillance—however, highly privacy protective tools, such as the Apple-Google exposure notification API, may be able to be used by higher-risk governments yet pose a low risk of adverse human rights impacts.

  - **Keep in mind the highly contextual nature of public health emergencies.**

The same solution will work differently and have different human rights impacts in different contexts. Companies should look to lessons learned from the humanitarian data sector and engage with the humanitarian community to benefit from their expertise in addressing emergency situations in a wide variety of contexts.[10]

- **Only work with the appropriate government authorities for a public health emergency.** This may differ somewhat from country to country, and non-traditional entities such as ministries of technology or communication may be legitimately involved. However, under no circumstances should a company work with security services, law enforcement, or intelligence entities—these entities are always high risk regardless of the country context, and should therefore be avoided in public health emergency-related business deals.

- **Avoid open-ended projects.**
  When possible, companies should set time limits or sunset clauses in contracts with government entities, review for compliance, and decide whether the contract should be continued at appropriate intervals.

ENABLE: HOW COMPANIES SHOULD WORK WITH OTHERS

» **Be as transparent as possible.**
Companies should publicly disclose how they are contributing to a public health emergency response. This includes:

- **Contract transparency.**
  Disclose which entities the company is working with, as well as the details of government requests, such as RFPs.

- **What kinds of data is being used, how, and what privacy protections are in place**.
  Both data subjects and the public at large have the right to know how their data is being used to respond to public health emergencies, as well as how companies are protecting their privacy and preventing their data from falling into the wrong hands.

- **What the company has decided not to do.**
  If the company has decided it will not pursue work in a given area or has established relevant principles or redlines, it should publicly disclose that information.

- **Maintaining records for audits.**
  Investigations by data protection authorities about the use of personal data are likely to take place after the emergency is over, and companies should be prepared.

» **Ensure all appropriate stakeholders are at the table.**
Stakeholder engagement is a key element of corporate human rights due diligence, and it is arguably even more important during public health emergencies. Although events may move fast, companies should still consult with appropriate stakeholders to ensure they are making fully informed decisions and avoiding serious human rights oversights. Relevant stakeholders for

[10] For example, the humanitarian sector has a long history of working closely with governments and has developed guidance on public-private partnerships that are also relevant for companies in public health emergencies. See https://centre.humdata.org/guidance-note-data-responsibility-in-public-private-partnerships.

public health emergencies could include public health authorities, independent health, medical, and scientific experts, civil society, and members of vulnerable groups, among others.

» **Ensure that engagements with government customers avoid misuse or abuse of product, service, or data sharing arrangement.**
Over-broad government requests or over-ambitious company offerings may lead to scope creep, misuse or abuse of a product, service, or data sharing arrangement. To avoid this, companies should work closely and deliberately with government customers. Companies should ensure government entities have the capacity and technology literacy required and that they understand the human risks involved. This should include clear guidance on purpose limitation and involve regular follow-ups over time to ensure things are on track.

» **Engage with other companies to establish rights-based redlines and set standards.**
In cases where government overreach is widespread, more than one company will likely be implicated. Companies can work together to prevent overreach by establishing rights-based redlines on the types of data they will share, with which entities, and for what purpose, and collectively challenge governments when needed. They can also collaborate to establish both technical and policy standards for commonly used tech solutions, such as contact tracing apps, while at the same time avoiding anti-competitive practices and consequences. Industry groups can help create leverage and avoid a race to the bottom. In cases where there is widespread concern about company conduct, or system-wide human rights risks to mitigate, companies can collaborate on joint position statements—in the context of COVID-19, for example, several pharmaceutical companies released a statement saying they will not rush vaccine development.

» **Pursue partnerships to proactively advance public health.**
Companies have an opportunity to take actions that promote the enjoyment, realization, and fulfillment of human rights, including the right to health and science, through the use of technology and data. Companies should seek to learn from past experiences and create a strong foundation for addressing future public health emergencies. This might include establishing long-term partnerships to advance a goal of continued relevance, as well as establishing and maintaining relevant relationships to prepare companies' to better respond to the next crisis.

INFLUENCE: HOW COMPANIES SHOULD INFLUENCE PUBLIC POLICY

» **Advocate for rights-respecting approaches to dealing with public health emergencies.**
As governments come to companies with various requests, companies have an opportunity to advocate for rights-respecting approaches and push back on requests that unduly limit rights. Companies should exchange lessons learned and best practices with other companies, and advocate for relevant standards or regulations that can provide clarity on the line between privacy and public health. They should also push for stronger health data regulations that include non-traditional health data.

» **When required by a government to share data beyond what is necessary and proportionate, push back as much as possible.**
The GNI Principles provide direction for how companies should address government demands, laws, or regulations that do not adhere to internationally recognized human rights standards.

7. COVID-19 Case Studies and Lessons Learned from Past Emergencies

COVID-19 CASE STUDIES

Although COVID-19 remains an active global public health emergency, there are already a number of lessons that can be learned from how various countries have utilized emergency powers, as well as different approaches to technology and data use for pandemic response. Below we examine three cases: the abuse of emergency powers in Hungary, India's use of a tech solution that exacerbated the digital divide, and South Korea's digitally driven response that has raised important questions about proportionality.

Hungary and the Abuse of Emergency Powers

Hungary has made headlines for its drastic expansion of emergency powers. To address COVID-19, the government declared a "state of danger" and then instituted the Coronavirus Defense Act in April 2020. Although the Hungarian Constitution states that emergency laws can only be in effect for 15 days, the Coronavirus Defense Act allows the government to issue decrees with no sunset clause. It also allows the government to issue decrees nearly without limit, and has resulted in decrees that have nothing to do with the pandemic, such as those related to restricting the rights of local governments.[11]

Several of the emergency decrees have unduly limited the right to privacy. First, the government issued a decree suspending various provisions of the GDPR, a move that received criticism from the European Data Protection Board. Another decree allows two Hungarian state bodies—the Ministry of Innovation and the pandemic advisory board—to access any kind of personal data. Once the initial "state of danger" ended, this emergency decree became law.

Despite being a member of the European Union and subject to the GDPR, several factors enabled the Hungarian government to abuse its emergency powers and derogate human rights in ways that are neither necessary nor proportionate. First, Hungary's Data Protection Authority was not independent, as DPAs are meant to be. Second, condemnation from the European Data Protection Board also came too slowly. Emergency powers operate much more quickly than the normal speed of government. And finally, Hungarian companies have little recourse to push back. Many require partnership and support from the government for their license to operate, and they therefore cannot serve as a check on the government to prevent indiscriminate data sharing and privacy violations.

India and the Digital Divide

Central to India's COVID-19 response is the contact tracing app Aarogya Setu, which raised numerous concerns around transparency, privacy, efficacy, and accountability. When it was first introduced in April 2020, the government made it mandatory for all government and private sector employees to download the app. One Indian state also announced that non-compliance in downloading the app

[11] Expert interview with BSR.

would lead to a criminal penalty. Given less than 40 percent of Indians have access to smartphones, the government's compulsory measure was also deemed exclusionary.

Because the government-mandated app was not accessible by the majority of the population, this measure disproportionately affected individuals' right to work, freedom of movement, and health. In a country with a deep digital divide, technology solutions alone cannot be the solution to improve public health outcomes. Following concerns expressed by civil society, the government announced in June that the app was no longer mandatory. To increase access to contact tracing, the government later made a similar version of the app available to people with landline phones.

The government's contact tracing measures also raised concerns around data privacy. Aarogya Setu relies on the collection of location data, movement data, as well as other personal data such as whether the individual is a smoker or not. The government said that all data would be anonymized and protected; however, India does not have a national privacy law, a data protection authority, or a good track record on data privacy. Other concerns include the opaque and ambiguous involvement of tech companies in the development of the app, and the potential back-end connection to India's Aadhaar database that is known to include citizens' biometric information.

South Korea and the Question of Proportionality

South Korea's response to COVID-19 has been widely applauded as a success as they quickly managed to flatten the curve and limit the number of fatalities. Their 3T strategy (Test, Trace, Treat) relied heavily on the use of technology solutions and data. The legal and policy context that permitted this was largely shaped after the country's experience with the MERS outbreak in 2015. Amendments made to the Contagious Disease Prevention and Control Act after the MERS outbreak allowed authorities to override certain provisions of Korea's stringent data privacy laws.

Korea's integrated contact tracing system relies on both "front-end" and "back-end" systems, and the collection of seven different types of data: mobile phone location data collected from telecommunications companies; personal identification information; medical and prescription records; immigration records; card transaction data for credit, debit, and prepaid cards; transit pass records for public transportation; and closed circuit television (CCTV) footage. For infected individuals, this data is not only shared across government agencies, but also disclosed publicly to citizens through text messages sent by health authorities and local governments. A typical "safety guidance text" would include a list of locations an infected individual visited before they were hospitalized. Privacy concerns were raised as individuals' private lives were shared as public information. Individuals were subject to online harassment for their sexual preferences or the activities they engaged in. In some cases, infected individuals were allegedly reidentified. Restaurants or shops visited by infected individuals often experienced an abrupt loss of business.

Following civil society concerns and recommendations by Korea's National Human Rights Commission, which stated that "the revelation of exceedingly detailed information was unwarranted," health authorities limited the scope and detail of information that was disclosed. The case of South Korea has

shown how integrated IT systems can enable a quick and effective response to the pandemic. It has also shown how non-traditional health data might be helpful for health authorities.

On the other hand, there are significant questions about proportionality of such measures. While there is no question that South Korea has avoided the scale and severity of COVID-19 impacts suffered by much of the world, there are questions about whether the large amount of personal information that was collected and disclosed was necessary. Further research on the effectiveness of such measures is needed to assess the necessity and proportionality of such measures, and effective technology solutions should be balanced with privacy protections.

CASE STUDIES FROM PAST EMERGENCIES

Although the COVID-19 pandemic is pathbreaking in terms of the scale of the crises and the widespread use of technology and data-based solutions, there are useful lessons to be found in examining past global emergencies, both public health related and not. Below we review two case studies of relevance to technology and data use in public health emergencies and the resulting impacts on human rights: the digitization of disease response during the 2014 Ebola outbreak in West Africa and the 2015 MERS outbreak in South Korea, and the expansion of global surveillance post-9/11.

The Digitization of Disease Response: The 2014 Ebola Outbreak of West Africa and the 2015 MERS Outbreak of South Korea

The use of data in response efforts to both the 2014 Ebola outbreak and the 2015 MERS outbreak was unprecedented for public health crises. During the MERS outbreak, the South Korean government collected mass amounts of personal information from mobile network operator databases to impose quarantine on people based on probabilities of infection. These algorithms were used to preemptively restrict movements of thousands of people without direct evidence of infection.

During the Ebola outbreak in West Africa, emergency powers were largely outsourced to the humanitarian sector, which invested resources into the region to experiment with new technologies. International organizations introduced a huge number of information systems rapidly and without sufficient forethought—one group reported 300 separate initiatives to engage the public. The humanitarian sector also called on mobile network operators to share Call Detail Records (CDRs) with governments, businesses, and international organizations for contact tracing purposes.

- **Evidence of efficacy is needed to determine the necessity and proportionality of an intervention.** Assessing the impact of interventions and being transparent about the results is key to avoid repeating the same mistakes. Good intentions should not replace justifications of necessity during a crisis—we need to know the benefits of an intervention (e.g. whether using CDR data for contact tracing works) and its possible consequences (e.g. other ways the government can use CDRs) to be able to assess proportionality. Unfortunately, the efficacy of contact tracing using CDRs was never properly documented and evaluated. If we had evidence that using CDR data helped for MERS and Ebola, we could better assess the necessity or proportionality of this same intervention for COVID.

- **Stronger data protections and data governance structures are needed for humanitarian and emergency response.** Public health authorities can learn from the humanitarian data

field—this is especially true in the Global South where data protection regulations might not be as strong. The humanitarian data field has made significant advancements in responsible data governance, and best practices include the work of the UN OCHA Centre for Humanitarian Data[12] and the International Committee of the Red Cross[13]. These principles and practices are relevant for data use during emergencies in all contexts, not just the humanitarian field.

Emergency Measures that Outlast the Emergency: 9/11 and the Entrenchment of the Modern Surveillance State

In the time since the 9/11 attacks in 2001, governments have accelerated attempts to anticipate and predict terrorist threats with a view to eradicate the capabilities of terrorists and prevent terror attacks. This has been a global effort that has resulted in the normalization of enormous domestic and foreign data-collection and surveillance activities by many governments. Three key lessons can be drawn from the experience of how the fight against terrorism has developed since 2001 that are highly relevant to the context of public emergencies:

» **Government overreach during times of emergency is likely.** Through national legislation, states have created their own definitions of terrorism in the absence of a commonly agreed approach. This has led to broad and vague classifications that have been used to attack political opponents and challenge the legitimate right to protest. For example, President Rodrigo Duterte recently signed an anti-terror law in the Philippines giving security forces "the power to arrest activists, journalists, and social media users by simply saying they are suspected of terrorist activities".

  In 2013, the Snowden revelations shone a spotlight on the global surveillance capabilities of the U.S. and U.K. governments and use of secrecy obligations to limit companies' ability to speak out. Some activities of the U.S. and U.K. governments have subsequently been found to be unlawful. The recent Schrems II ruling by the Court of Justice of the European Union (CJEU) focused on the adequacy of data transfer agreements between the U.S. and E.U. to meet data protection standards is one of many ongoing fallouts from the Snowden revelations. In the context of the current COVID-19 pandemic, some governments (for example, Hungary) are using the context of the emergency to govern by decree in a way that bypasses fundamental rights guarantees.

» **Governments increasingly outsource surveillance activities to the private sector.** Key aspects of the war on terror have been outsourced through legislation to the private sector. For example, for policing customers and transactions for terrorism financing, obligations to collect and disclose data (such as passenger and ISP data), and positive disclosure obligations regarding suspicions of terrorism. COVID-19 is accelerating a similar process not only for public health but elsewhere too—for example, obligations on the hospitality industry to collect data on all customers.

[12] See https://centre.humdata.org/wp-content/uploads/2019/03/OCHA-DR-Guidelines-working-draft-032019.pdf and https://centre.humdata.org/guidance-note-data-responsibility-in-public-private-partnerships.
[13] See https://www.icrc.org/en/data-protection-humanitarian-action-handbook.

» **Oversight and transparency are essential, but difficult to secure.** Civil society and human rights expertise are either absent or marginalized from the infrastructure that has been developed to fight terrorism over the last 20 years. This is despite a body of evidence showing that measures taken in the fight against terrorism have negatively impacted rights and freedoms around the world, and can fuel grievances and conflict that increase the risk of terrorism. National security is often cited as a reason for curtailing public interrogation of counter-terrorism activities, and in the context of public health emergencies, the speed of action required to tackle a pandemic is now similarly given as a reason to limit legislative / parliamentary oversight of coronavirus restrictions. It is essential that companies have a proactive strategy of transparency with the public about the role they are playing in the pandemic, and push to be more transparent where they are prevented from being so.

8. Conclusion and Areas for Further Inquiry

We expect a future with more public health emergencies and greater company involvement in addressing them.

In this context, companies should be prepared to make human rights-based business decisions in the complicated context of public health emergencies to avoid unduly infringing on other human rights in the name of protecting public health, and to prevent invasive emergency measures from becoming permanent. The ideas discussed in this paper and the human rights framework for business decisions in public health emergencies are one contribution toward that end. However, several questions and challenges remain that merit further exploration.

First, there is not enough evidence of what technology and data-based solutions work and what do not. Because widespread use of data and technology-based solutions to public health emergencies is still relatively new and many systems are hastily assembled with no mechanism for analyzing their efficacy, it is still unclear where specific lines around data collection should be drawn. This makes it challenging to effectively evaluate the necessity and proportionality of these activities.

Second, it is unclear to what extent emergency measures are needed to address public health crises. This is partially due to the lack of clear guidance from international human rights bodies about the particularities of public health states of emergency. As Nina Sun argued, a general comment on derogations for public health reasons that provides specific guidance to address the necessity and proportionality of state responses and the misuse of emergency powers would provide much needed clarity to the nuances of public health-related human rights derogations.

Third, while there has already been significant examination of the erosion of privacy that comes with the entrenchment of state of emergency surveillance systems, privacy is far from the only human right impacted. With the expansion of connectivity and the proliferation of artificial intelligence and internet of things, tech and data-based responses to future public health emergencies have the potential to have significant impacts on various aspects of human freedom and agency in unanticipated ways.

Finally, companies have a significant opportunity to use data and technology-based solutions to help fulfill human rights. While many companies feel a moral obligation to help fulfill the right to health during public health crises, there is no framework for them to do so because there is no corporate responsibility to promote human rights according to the UNGPs. It is also unclear whether businesses have a responsibility to protect the right to health during public health emergencies when governments are not doing enough. BSR believes companies have an important role to play in the creation of an enabling environment for human rights, including the advancement of public health and the fulfillment of the right to science. However, the promotion of human rights does not detract from (and cannot be used to offset) the responsibility to prevent and mitigate risks to other rights.

About BSR

BSR is a global nonprofit organization that works with its network of more than 250 member companies and other partners to build a just and sustainable world. From its offices in Asia, Europe, and North America, BSR develops sustainable business strategies and solutions through consulting, research, and cross-sector collaboration. Visit www.bsr.org for more information about BSR's 25 years of leadership in sustainability.

www.bsr.org

BSR®