

GLOBAL DIGITAL POLICY SNAPSHOT

Democratic Responses to the Pandemic & Digital Rights

JULY 2020

KEY TAKEAWAYS

Challenge: In response to the COVID-19 crisis, governments around the world have enacted emergency regulations and deployed new digital technologies, as they struggle to protect public health. The challenge for democracies is to combat the disease vigorously without unnecessarily undermining core civil and political rights.

State of Play: Governments have deployed digital surveillance tools and contact tracing apps, and enacted laws criminalizing misinformation about the disease or limiting access to information, without considering human rights impacts or putting adequate privacy and civil liberties checks in place. As a consequence, a wide range of human rights have been put at risk, including the right to privacy, access to information, and the freedoms of movement, assembly, and expression.

Recommendations: This brief identifies four safeguards for policymakers, as they contemplate emergency regulations and application of digital technologies in response to COVID-19. Policymakers should:

- Assess the efficacy of digital technology for public health purposes before deploying;
- Evaluate all emergency regulations and newly deployed digital technologies for consistency with international human rights law;
- Incorporate meaningful checks and limitations on emergency powers and newly deployed technologies, such as sunset clauses, restrictions on use of data, and independent oversight structures; and
- Communicate objectives, rationale, and risks of emergency measures transparently to citizens.

INSIDE THIS BRIEF:

- *Landscape of Government Responses to COVID-19*
- *Human Rights Implications and Risks*
- *Recommendations for Policymakers*
- *Diving Deeper on Government Responses to COVID-19*

INTRODUCTION

Governments around the world have enacted a wide range of emergency measures and deployed new digital technologies in response to the COVID-19 pandemic, but often without adequate consideration of the impacts on human rights. While the adoption of some of these measures may have been warranted and justifiable in the context of a global crisis, international human rights law requires that infringements on fundamental rights must be assessed with reference to whether they are necessary to accomplish a legitimate aim, proportional to the threat, and legal. Many governments have failed to undertake this analysis.

The combination of emergency regulations and deployment of digital tools to combat the spread of the virus or to help enforce the regulations have had significant consequences for human rights globally. Responses to the pandemic have included the criminalization of misinformation or inhibiting access to information about the disease, as well as government pursuit of expansive digital tracing, surveillance and monitoring capabilities without meaningful checks or limits on powers. Digital tools and data collection efforts present particular risk in this context. Social media monitoring for public health purposes can be readily turned to the purpose of monitoring dissenting voices and protest activities. And digital surveillance methods such as location tracking or facial recognition technologies employed to combat the pandemic's spread can be appropriated by law enforcement or immigration agencies to serve far more expansive and enduring objectives.

The pandemic has led to a dramatic shift in reliance on tools for virtual engagement, particularly as borders and offices have closed across the globe and citizens are increasingly using digital technologies to stay connected and productive. As these tools become ever more ubiquitous in daily life, and as new technologies present governments with powerful capabilities in the public health context, it is critical that democratic governments recognize—and act to ensure—that obligations to protect human rights extend fully to the digital realm.

LANDSCAPE OF GOVERNMENT RESPONSES TO COVID-19

Ongoing research by the International Center for Not-for-Profit Law (ICNL) indicates that at least 88 governments have declared an emergency situation in response to COVID-19. Many more have invoked preexisting disaster and emergency measures that affect civic freedoms. The responses have been implemented by democracies and autocracies alike, with particular implications for the right to privacy; the freedoms of assembly, movement and expression; and access to information.

Over 40 governments have implemented measures that affect the **right to privacy** through the introduction of digital proximity and contact tracing tools, often without foundation in the legislative process. Tracking technology can support laborious contact tracing efforts and help contain infection clusters, if carefully designed. Many apps, however, currently collect, share and save information without clear relation to tackling infections and without minimization standards or safeguards to limit the data's use to legitimate purposes. In the United Kingdom and Poland, personal data is saved in central databases without firewalls or limitations regarding which government agencies have access, raising concerns about the use of data for purposes other than combatting the pandemic. Additionally, many tracing apps have not been efficacious—suggesting a failure of governments to evaluate the effectiveness of technology-driven responses in advance. Singapore's government is now in the process of introducing mandatory wearable bluetooth devices, a push that could signal a trend towards continuous, obligatory tracking that would implicate the need for new protections of privacy rights.

A growing number of governments are also requesting access to telecommunications data and location information, with direct implications for **freedoms of assembly and movement**. In Armenia, for example, telecommunications companies are required to provide authorities with their customers' phone records, including phone numbers and the location, time, and date of their calls and text messages; however, the government has not communicated how this information will help authorities identify people with COVID-19. Slovakia's authorities have had access to telecom data for the purposes of contact tracing since March, and similar approaches have been introduced in Israel and are planned in the Netherlands. In other cases, introduction of new COVID-related tools risks deepening existing surveillance regimes. In India, many are concerned that the tracing app could become a tool of mass surveillance for a government with an already concerning record of trampling civil liberties. Some countries, such as Poland, are using facial recognition technology to enforce stay at home orders. The rights implications of such expansive and intrusive measures were underlined by the constitutional court in Slovakia, which declared parts of the phone-tracking law unconstitutional, citing insufficiently clear intentions and lacking guarantees against potential misuse of personal data.

ICNL has also tracked over 40 countries with measures that affect **freedom of expression**. Under the pretense of targeting misinformation around COVID-19, more than a dozen countries have enacted harsh criminal penalties for sharing particular categories of content online. Others have ratcheted up enforcement of “fake news” laws to penalize criticism of the government's response. Argentina equipped its security forces to carry out so-called cyber patrols and prosecute users of social networks for “public intimidation” about COVID-19 online, without clarity about what constitutes intimidation. Even democratic governments are chilling free expression, shielding themselves from criticism while penalizing dissent. In Botswana, a person can spend five years in prison for intentionally deceiving someone on social media about COVID-19. Some governments have exhibited restraint in this area only after meeting civil society resistance, such as in Tunisia and Bulgaria, where lawmakers withdrew bills that aimed to criminalize spreading misinformation following widespread protests.

More than 25 governments have also restricted **access to information**, an important prerequisite for the exercise of freedom of expression. Government officials in Brazil and Georgia are not required to answer any freedom of information requests during the state of emergency. Other governments aim to control access to information about COVID-19 online. In the Indian Maharashtra region, publishing information about the virus on social media without prior clearance from the government is a punishable offense. While access to accurate information about government responses is important in emergency situations, these measures will deter individuals from sharing what could be valuable information and limit the possibilities to hold governments accountable.

HUMAN RIGHTS IMPLICATIONS & RISKS

In the COVID-19 context, some extraordinary digital measures may be legitimate, even though they impinge on the full exercise of several civil liberties. As a threshold matter, however, governments must undertake a meaningful assessment of the effectiveness of digital technologies in achieving legitimate public health objectives. If the technology doesn't serve a public health purpose there is no justification for putting rights at risk. If the technology can be integrated effectively in pandemic responses--meeting a baseline test of efficacy--the next responsibility of governments is to move on to a human rights assessment.

In employing emergency measures--including emergency restriction on liberties, collection of data, and deployment of digital tools--governments are responsible for substantively assessing whether rights and liberties will be implicated by their actions. Where infringement occurs, human rights law provides a framework for determining whether the actions are justifiable. Built into each of the core civil and political liberties enshrined in the International Covenant on Civil and Political Rights (ICCPR, the primary international treaty on these rights) are requirements for restrictions of these rights in certain, limited situations. As interpreted and applied, restrictions are permitted only where they are (1) **necessary** to achieve a **legitimate** government purpose, such as protecting national security and public safety (or in this instance, public health) for a **limited period**; (2) **proportionate** to the threat that's being addressed; and (3) compliant with the **legality** principle, which requires public notice and sufficient clarity to enforce the restrictions transparently.

Even in times of emergency, states are limited in their ability to act outside their human rights obligations. Article 4 of the ICCPR permits a temporary derogation, under requirements that mirror those described above. However, in responding to this pandemic, many democratic governments have failed to substantively evaluate their actions' impact on human rights, and to ensure that measures that derogate civil and political rights are appropriately tailored to satisfy the principles of necessity, proportionality, and legality.

While enacting intrusive measures--such as digital surveillance and expanded police powers--many governments have neglected to incorporate narrowing provisions, such as sunset clauses, data minimization standards, or additional safeguards to ensure measures are limited to legitimate purposes.

In addition to incorporating these rights protections into emergency regulations, governments must similarly assess relevant technologies to ensure alignment with these human rights principles. The MIT Technology Review has, for example, developed a methodology for evaluating government tracking apps, including assessments of whether the app is voluntary and whether the use and collection of data are subject to minimization standards, among other considerations. Such normative assessments can help governments ensure that appropriate rights protections are accounted for in the deployment of digital technologies.

Finally, democratic governments bear the responsibility of transparently communicating the rationale for restrictions on liberty to citizens. When citizens' health is at stake, many will understand and support restrictions to their individual rights as long as they know and understand why measures are taken. While transparency is not itself a justification for emergency-inspired restrictions, this is an important aspect of how democratic governments build trust, and how they differentiate themselves from authoritarian rulers.

The risks presented by these emergency responses--and their application of digital technologies--are compounded by a wider atmosphere of dwindling confidence in democracies. Authoritarian governments boasting of the purported superiority of their response to the pandemic threaten to exacerbate pressure on democracies and may tempt policymakers to ignore their human rights commitments in the name of efficiency.

Governments must demonstrate that emergencies can be tackled by leveraging digital technologies while protecting and promoting human rights. Moreover, if democratic governments fail to engage in human rights assessments of their own digital tools and accompanying regulations, or to include reasonable checks on their own emergency powers, it is hard to criticize authoritarian governments for deliberately ignoring their legal obligations.

RECOMMENDATIONS FOR POLICY MAKERS

To safeguard the rights of citizens, policymakers in democratic governments should:

1. **Assess the efficacy of digital technology for public health purposes before deploying.** Prior to introducing digital tools that may have implications for citizens' rights, governments should conduct assessments of whether deploying digital technology will be effective at advancing legitimate public health objectives.
2. **Evaluate all emergency regulations and newly deployed digital technologies for consistency with international human rights law.** Governments must both substantively evaluate the impact of emergency measures on citizens' rights and liberties, and ensure any derogation or restriction of rights is consistent with principles of necessity, proportionality, and legality.
3. **Incorporate meaningful checks and limitations, such as independent oversight, on emergency powers and authorities.** Policymakers should expressly include limits on emergency measures, such as sunset clauses; narrow minimization standards for the collection of data; and restrictions on the appropriate use and storage of collected data and health information. Measures should be subject to oversight and review by a legislative or independent authority to evaluate effectiveness and ensure ongoing alignment with a rights-based democratic governance model.
4. **Communicate objectives, rationale, and risks of emergency measures transparently to citizens.** Policymakers should ensure the public can understand the government's actions--and the ways and extent to which citizens' rights may be impacted--as a means of building trust and differentiating emergency measures from authoritarian opportunism.

DIVING DEEPER ON GOVERNMENT RESPONSES TO COVID-19

COVID-19 Civic Freedom Tracker, International Center for Not-for-Profit Law.

The COVID-19 Test of Democratic Governance, Eileen Donahoe, *The American Interest*.

Democracy Versus the Pandemic, Larry Diamond, *Foreign Affairs*.

Pandemics and Human Rights, Doug Rutzen and Nikhil Dutha, *Just Security*.

COVID-19: The Surveillance Pandemic, Lisa Vermeer, Zach Lampell, & Nicholas Miller, *ICNL*.

AUTHORS

Eileen Donahoe is Executive Director of the Global Digital Policy Incubator. She previously served as the U.S. Ambassador to the UN Human Rights Commission, and serves in leadership and advisory roles across the global democracy and human rights community.

Lisa Vermeer is a Digital Policy Advisor at ICNL. She is advancing ICNL's work addressing the impact of digital technology on civil society and human rights. She is a political scientist focusing on the intersection of technology, policy and society. Lisa has advocated for human rights online on behalf of the Ministry of Foreign Affairs of the Netherlands.

Kip Wainscott is a Senior Advisor for the Global Digital Policy Incubator. A lawyer and policy professional with experience in government, civil society, and the private sector, he has worked extensively on issues concerning technology's impact on democracy and human rights.

This snapshot was created in
partnership with the International
Center for Not-for-Profit Law.

ICNL
INTERNATIONAL CENTER
FOR NOT-FOR-PROFIT LAW