

Joint civil society statement: States use of digital surveillance technologies to fight pandemic must respect human rights

2 April 2020

The COVID-19 pandemic is a global public health emergency that requires a coordinated and large-scale response by governments worldwide. However, States' efforts to contain the virus must not be used as a cover to usher in a new era of greatly expanded systems of invasive digital surveillance.

We, the undersigned organizations, urge governments to show leadership in tackling the pandemic in a way that ensures that the use of digital technologies to track and monitor individuals and populations is carried out strictly in line with human rights.

Technology can and should play an important role during this effort to save lives, such as to spread public health messages and increase access to health care. However, an increase in state digital surveillance powers, such as obtaining access to mobile phone location data, threatens privacy, freedom of expression and freedom of association, in ways that could violate rights and degrade trust in public authorities – undermining the effectiveness of any public health response. Such measures also pose a risk of discrimination and may disproportionately harm already marginalized communities.

These are extraordinary times, but human rights law still applies. Indeed, the human rights framework is designed to ensure that different rights can be carefully balanced to protect individuals and wider societies. States cannot simply disregard rights such as privacy and freedom of expression in the name of tackling a public health crisis. On the contrary, protecting human rights also promotes public health. Now more than ever, governments must rigorously ensure that any restrictions to these rights is in line with long-established human rights safeguards.

This crisis offers an opportunity to demonstrate our shared humanity. We can make extraordinary efforts to fight this pandemic that are consistent with human rights standards and the rule of law. The decisions that governments make now to confront the pandemic will shape what the world looks like in the future.

We call on all governments not to respond to the COVID-19 pandemic with increased digital surveillance unless the following conditions are met:

1. Surveillance measures adopted to address the pandemic must be lawful, necessary and proportionate. They must be provided for by law and must be justified by legitimate public health objectives, as determined by the appropriate public health authorities, and be proportionate to those needs. Governments must be transparent about the measures they are taking so that they can be scrutinized and if appropriate later modified, retracted, or overturned. We cannot allow the COVID-19 pandemic to serve as an excuse for indiscriminate mass surveillance.
2. If governments expand monitoring and surveillance powers then such powers must be time-bound, and only continue for as long as necessary to address the current pandemic. We cannot allow the COVID-19 pandemic to serve as an excuse for indefinite surveillance.
3. States must ensure that increased collection, retention, and aggregation of personal data, including health data, is only used for the purposes of responding to the COVID-19 pandemic. Data collected, retained, and aggregated to respond to the pandemic must be limited in scope, time-bound in relation to the pandemic and must not be used for commercial or any other purposes. We cannot allow the COVID-19 pandemic to serve as an excuse to gut individual's right to privacy.

4. Governments must take every effort to protect people's data, including ensuring sufficient security of any personal data collected and of any devices, applications, networks, or services involved in collection, transmission, processing, and storage. Any claims that data is anonymous must be based on evidence and supported with sufficient information regarding how it has been anonymized. We cannot allow attempts to respond to this pandemic to be used as justification for compromising people's digital safety.
5. Any use of digital surveillance technologies in responding to COVID-19, including big data and artificial intelligence systems, must address the risk that these tools will facilitate discrimination and other rights abuses against racial minorities, people living in poverty, and other marginalized populations, whose needs and lived realities may be obscured or misrepresented in large datasets. We cannot allow the COVID-19 pandemic to further increase the gap in the enjoyment of human rights between different groups in society.
6. If governments enter into data sharing agreements with other public or private sector entities, they must be based on law, and the existence of these agreements and information necessary to assess their impact on privacy and human rights must be publicly disclosed – in writing, with sunset clauses, public oversight and other safeguards by default. Businesses involved in efforts by governments to tackle COVID-19 must undertake due diligence to ensure they respect human rights, and ensure any intervention is firewalled from other business and commercial interests. We cannot allow the COVID-19 pandemic to serve as an excuse for keeping people in the dark about what information their governments are gathering and sharing with third parties.
7. Any response must incorporate accountability protections and safeguards against abuse. Increased surveillance efforts related to COVID-19 should not fall under the domain of security or intelligence agencies and must be subject to effective oversight by appropriate independent bodies. Further, individuals must be given the opportunity to know about and challenge any COVID-19 related measures to collect, aggregate, and retain, and use data. Individuals who have been subjected to surveillance must have access to effective remedies.
8. COVID-19 related responses that include data collection efforts should include means for free, active, and meaningful participation of relevant stakeholders, in particular experts in the public health sector and the most marginalized population groups.

Signatories:

7amleh – Arab Center for Social Media Advancement
Access Now
African Declaration on Internet Rights and Freedoms Coalition
AI Now
Algorithm Watch
Alternatif Bilisim
Amnesty International
ApTI
ARTICLE 19
Asociación para una Ciudadanía Participativa, ACI Participa
Association for Progressive Communications (APC)
ASUTIC, Senegal
Athar - Freedom of Expression Activist Organization

Australian Privacy Foundation
Barracón Digital
Big Brother Watch
Bits of Freedom
Center for Advancement of Rights and Democracy (CARD)
Center for Digital Democracy
Center for Economic Justice
Centro De Estudios Constitucionales y de Derechos Humanos de Rosario
Chaos Computer Club - CCC
Citizen D / Državljan D
CIVICUS
Civil Liberties Union for Europe
CódigoSur
Coding Rights
Coletivo Brasil de Comunicação Social
Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
Comité por la Libre Expresión (C-Libre)
Committee to Protect Journalists
Consumer Action
Consumer Federation of America
Cooperativa Tierra Común
Creative Commons Uruguay
D3 - Defesa dos Direitos Digitais
Data Privacy Brasil
Democratic Transition and Human Rights Support Center "DAAM"
Derechos Digitales
Digital Rights Lawyers Initiative (DRLI)
Digital Rights Watch
Digital Security Lab Ukraine
Digitalcourage
EPIC
epicenter.works
European Digital Rights - EDRi
Fitug
Foundation for Information Policy Research
Foundation for Media Alternatives
Fundación Acceso (Centroamérica)
Fundación Ciudadanía y Desarrollo, Ecuador
Fundación Datos Protegidos
Fundación Internet Bolivia
Fundación Taigüey, República Dominicana
Fundación Vía Libre
Hermes Center
Hiperderecho
Homo Digitalis
Human Rights Watch
Hungarian Civil Liberties Union
ImpACT International for Human Rights Policies
Index on Censorship

Initiative für Netzfreiheit
Innovation for Change - Middle East and North Africa
International Commission of Jurists
International Service for Human Rights (ISHR)
Intervozes - Coletivo Brasil de Comunicação Social
Ipandetec
IPPF
Irish Council for Civil Liberties (ICCL)
IT-Political Association of Denmark
Iuridicum Remedium z.s. (IURE)
Karisma
La Quadrature du Net
Liberia Information Technology Student Union
Liberty
Luchadoras
Majal.org
Masaar "Community for Technology and Law"
Media Rights Agenda (Nigeria)
MENA Rights Group
Metamorphosis Foundation
New America's Open Technology Institute
Observacom
Open Data Institute
Open Rights Group
OpenMedia
OutRight Action International
Pangea
Panoptykon Foundation
Paradigm Initiative (PIN)
PEN International
Privacy International
Public Citizen
Public Knowledge
R3D: Red en Defensa de los Derechos Digitales
RedesAyuda
SHARE Foundation
Skyline International for Human Rights
Sursiendo
Swedish Consumers' Association
Tahrir Institute for Middle East Policy (TIMEP)
Tech Inquiry
TechHerNG
TEDIC
The Bachchao Project
Unwanted Witness, Uganda
Usuarios Digitales
WITNESS
World Wide Web Foundation