COVID-19 Digital Rights Tracker

This live tracker documents new measures introduced in response to COVID-19 that pose a risk to digital rights around the world.

Samuel Woodhams
20 Mar 2020 14:30 GMT

UPDATED 09 April 16:30 GMT to include the latest digital tracking, physical surveillance and censorship measures.

Key Findings

In response to the outbreak of COVID-19:

- **New digital tracking measures** have been introduced in 23 countries
- **Advanced physical surveillance technologies** are in use in 9 countries
- **COVID-19-related censorship** has been imposed by 12 governments
- **Internet shutdowns** continue in 4 countries despite the outbreak

Introduction

Since the outbreak of COVID-19, governments around the world have implemented a range of digital tracking, physical surveillance and censorship measures in a bid to slow the spread of the virus.

Some of these may well be **proportionate, necessary and legitimate** during these unprecedented times. However, others have been rushed through legislative bodies and implemented without adequate scrutiny.

Over the coming weeks and months, this tracker will document new initiatives being deployed that could threaten digital rights to help stem overreach, promote scrutiny, and ensure that intrusive measures don't continue for any longer than absolutely necessary.

> To submit information regarding developments occurring around the world, please add details to this public Google Sheet.

The Google Sheet will be closely monitored and any initiatives that we have missed will be added to the report.

09/04/20 Update

In the first week of April, countries around the world have continued to implement digital tracking, physical surveillance and censorship measures in a bid to help stem the spread of the virus.

From electronic bracelets to track citizens in West Virginia, to the use of surveillance drones in New York, the US has significantly ramped up its response in recent weeks.

> In the past two weeks, we have documented 4 new initiatives that may pose a threat to citizens' digital privacy and civil liberties in the US.

Contact tracing apps continue to spread around the world and are likely to become even more pervasive once lockdown measures begin to be lifted.

There are currently contact tracing apps available in India, the US, Russia, Iceland and Singapore, among others. Many other health authorities, including in the UK, are in the process of developing their own apps.

However, the efficacy of these apps remains contested. According to the ACLU, for example: "None of the data sources [...] are accurate enough to identify close contact with sufficient reliability."

We have also seen an increase in the number of international initiatives, particularly in the EU.

Governments across Asia have implemented COVID-19-related censorship more than any other region, while European countries have introduced the most digital tracking measures.

Region	Digital Tracking	Censorship	Surveillance
Europe	10	0	3
Asia	9	7	3
MENA	2	3	1
SSA	1	2	0
N. America	2	0	3
S. America	3	0	0
Australasia	0	0	1

Regional breakdown of measures implemented in response to COVID-19

See previous updates

Country-by-Country Breakdown

Digital Tracking

As governments around the world implement measures to help slow the spread of the virus, many have turned to digital tracking initiatives to help monitor their populations.

Measures have included the use of aggregated mobile location data to track citizens during lockdowns, apps designed to help identify the location of those with the virus, and the deployment of advanced mobile monitoring technologies.

Below is a reverse chronological list of confirmed digital tracking measures being adopted around the world.

India – 05/04/20

On April 5, India Today reported the introduction of a new contact tracing app created by the Karnataka government.

According to the article, "the app aims to track the movement history of persons tested positive, before their detection in order to take precautions and to contain the coronavirus outbreak."

According to an article published the following day in Citizen Matters, "the governments of Kerala, Karnataka, Punjab and Tamil Nadu, the Ministry of Electronics and Information Technology (MeitY) and the National Informatics Centre (NIC) have released various mobile apps."

Rohini Lakshane writes that "while desperate times understandably call for desperate measures, many of these mobile phone-based interventions raise concerns about the privacy of users and that of persons directly affected by the novel coronavirus, overboard surveillance, and eventually, "function creep".

USA – 04/04/20

On April 4, CNN reported that two tech startups had tracked citizens visiting the beach in Fort Lauderdale, Florida, by monitoring mobile phone location data.

One of the companies involved then posted a heat map on Twitter to show their findings.

Despite claiming to only use anonymised data, it has been repeatedly been shown that even large anonymised data sets are at risk of re-identification.

Iceland – 02/04/20

Authorities in Iceland released a contact tracing app on April 2.

According to an article in the Iceland Review, the app "collects data about other phones in the area, making it easier to trace whom an individual was in contact with if they are later diagnosed with coronavirus."

At time of publication, the app was only available on the App Store.

Argentina – 30/03/20

At the end of March, the big data firm Grandata released a heat map showing the movement of citizens around Argentina to monitor compliance with new lockdown measures.

Privacy International have written: "this is the perfect example of the data exploitation industry and data brokers, using data that users probably where not aware they were sharing with third parties like Grandata"

USA – 28/03/20

According to a report by the Wall Street Journal on March 28: "Government officials across the U.S. are using location data from millions of cellphones in a bid to better understand the movements of Americans during the coronavirus pandemic."

"The data — which is stripped of identifying information like the name of a phone's owner — could help officials learn how coronavirus is spreading around the country and help blunt its advance," the story continues.

It is thought the data has been acquired from the mobile advertising industry, instead of mobile operators.

Brazil – 27/03/20

According to a report from ZDNet on March 27: "the mayor of Recife said the city is tracking at least 700.000 smartphones to identify where the lockdown rules are being followed"

The report continues: "Governments across Brazil are looking to roll out a system developed that uses geolocation tracking to support actions around the lockdowns intended to slow the spread of COVID-19."

The system is developed by InLoco, a Brazilian startup, and geotracks users "through a location map that doesn't use GPS or beacons, which InLoco claims to be 30 times more accurate than GPS."

Switzerland 26/03/20

According to a report by Reuters, "Switzerland has asked state-controlled Swisscom for day-old mobile phone data to help judge whether measures to restrict people's movements and slow the coronavirus's spread were working."

Daniel Koch, head of infectious diseases at the federal health agency, said it "it had nothing to do with [...] surveillance" as they were only acquiring data from the previous day.

South Africa – 24/03/20

On Wednesday 24 March, South Africa's communications minister Stella Ndabeni-Abrahams told reporters: "It is important to look at the individuals that are affected [by the virus] in order to be able to help the department of health to say that we know, in a particular area we have so many people that have been infected."

"The [telecommunications] industry collectively has agreed to provide data analytics services in order to help government achieve this," she continued.

According to a report by Business Insider, “She did not provide further details, and regulations that will govern South Africa’s national lockdown, and methods of curbing the spread of the virus, have not yet been published.”

Bulgaria – 24/03/20

According to a tweet from Dr. Vesselin Bontchev, from March 24 Bulgarian authorities will have the power to trace mobile phone traffic metadata and internet contacts without a court order.

According to his tweet, “The idea is to trace those in quarantine but this limitation is not spelled out in the law.”

Pakistan – 24/03/20

On March 24, Ramsha Jahangir reported that several residents across the country had received a text message alerting them that they may have come into contact with someone with the virus.

According to the article in Dawn, the message reads: “It has been observed that you may have come in contact with a confirmed coronavirus case in the last 14 days. You are, therefore, requested to take necessary precautionary measures by self-quarantine.”

It is thought the measure has been implemented via cell site location information (CSLI) and call detail record (CDR) data acquisition methods.

“Using CDR analysis, details such as locations visited by a confirmed Covid-19 patient as well as cell phone numbers of others who were in the same vicinity at the time can be obtained from the patient’s phone data,” the article continues.

Russia – 23/03/20

On March 23, the Russian government released an announcement ordering the Ministry of Communications to develop a new contact tracing system to help monitor citizens thought to have come into contact with those that have the virus.

According to Meduza, “the system [will] analyze specific individuals’ geolocation data from telecommunications companies.”

Singapore – 20/03/20

On March 20, a new app called TraceTogether was released by authorities in Singapore to help trace the spread of COVID-19.

The app, which already has 650,000 users according to the app's website, was developed by the Government Technology Agency and the Ministry of Health.

According to the Straits Times, the app can "identify people who have been in close proximity [...] to coronavirus patients using wireless Bluetooth technology."

According to a video released by TraceTogether, "No geolocation data or other personal data is collected."

India – 20/03/20

On Friday, 20 March, Reuters reported that: "People suspected of having the coronavirus in India have received hand stamps and are being tracked using their mobile phones and personal data."

The indelible hand stamps, which have been applied to citizens arriving at airports in Maharashtra and southern Karnataka, include the date that the person may be released from self isolation.

"In southern Kerala state, authorities have used telephone call records, CCTV footage, and mobile phone GPS systems to track down primary and secondary contacts of coronavirus patients," the Reuters story continues.

Poland – 19/03/20

On March 19, Poland's Ministry of Digital Affairs launched a new app for quarantined citizens.

The app prompts its users to send a geo-located selfie at random times throughout the day, so that authorities can ensure that they are abiding by the quarantine measures.

Failure to comply with the orders to remain inside could result in a fine of PLN 5,000.

According to Privacy International: "The system checks both the person (using facial recognition) and the location, essentially replicating what would otherwise be a visit from a police officer."

United Kingdom – 19/03/20

On Thursday March 19, Sky News reported that the British government was working with major mobile network, 02, to analyse its users' location data.

According to the article, "the project will not be able to track individuals and is not to designed to do so."

A report published the same day by The Guardian revealed that EE, the country's largest mobile operating company, was also in advanced discussions with the government about how best to share their users' location data.

As the article made clear, "privacy campaigners worry that handing over such personally identifying information in large quantities crosses a line that may be hard to step back from when things return to normality."

Hong Kong – 19/03/20

All international arrivals to Hong Kong currently have to stay at home for 14 days to help slow the spread of the virus. To track the new arrivals, authorities are now providing them with wristbands that log a user's location and share it with relevant authorities.

Anyone violating the quarantine orders could face up to six months in prison and a fine of up to HK$25,000, according to Quartz.

Italy – 18/03/20

Vodafone launched a five-point plan to help respond Oto the outbreak of COVID-19 on March 18.

According to the press release, the company was "already producing an aggregated and anonymous heat map for the Lombardy region in Italy to help the authorities to better understand population movements in order to help thwart the spread of COVID-19."

Israel – 17/03/20

On Tuesday, 17 March, Israel's government approved new surveillance measures that will allow the regime to track citizens by monitoring their mobile phones.

Benjamin Netanyahu had outlined his plans the previous weekend.

The technology, which was originally developed to assist in counter-terrorism operations, is thought to be able to track the physical location of all mobiles in the country, as well as monitor calls and messages.

According to digital rights group, 7amleh, it is also capable of accessing citizens cameras and headsets.

> Israel [is] committing mass violations of digital rights, especially the right to privacy, under the pretext of managing the health crisis caused by the Coronavirus. 7amleh

Ecuador – 17/03/20

According to a report by Ecuador TV, on March 17 Government Minister María Paula Romo announced that the government would begin to use satellite tracking to ensure citizens did not breach the "epidemiological fence."

Privacy International later reported that the measure "authorised tracking mobile phones via GPS satellite to ensure that citizens do not break mandatory quarantine after six violators were identified."

Germany – 17/03/19

Deutsche Telekom, the German mobile operator, announced on March 17 that it was passing anonymised location data of its users to the Robert-Koch Institute, a research institute and government agency responsible for disease control and prevention.

The move came after the government altered its GDPR-enabling legislation to allow the processing of personal data during an epidemic.

Austria – 17/03/20

In Austria, reports emerged on March 17 claiming that Austrian mobile operators had begun sharing anonymised mobile location data with the government.

Like the initiatives in Germany and the UK, the measure is intended to be used to track whether or not citizens' were restricting travel and following government advice.

South Korea – 16/03/02

On March 16, it was reported that Korean telecommunication companies and credit card companies were sharing data to the government to assist tracking the movement of its citizens.

It followed reports from earlier in the month that the government had launched an app to monitor citizens on lockdown to help contain the outbreak.

In a story byThe Guardian texts messages sent by health authorities and local district offices were also reportedly exposing "an avalanche of personal information and are fuelling social stigma."

Italy – 14/03/20

Like Germany, the UK and Austria, Italian mobile operators have also been shown to be sharing aggregated location data with health ministries.

In a bid to control the virus in a country that has now registered more Coronavirus-related deaths than China, the location data is thought to have to helped local authorities monitor citizens' responses to its lockdown measures.

According to a report by The Guardian, over 40,000 Italians have been found to be violating the lockdown measures.

Belgium – 12/03/20

On March 11, the Belgian government confirmed that it would allow local mobile operators to share anonymised data with a third party to help track the spread of the virus.

The following week, a group of technology entrepreneurs argued in favour of creating app to track and regulate individuals' movement based on their health status.

Iran – 03/03/20

On Tuesday, March 3, Iranian citizens received a notification about a new app supposedly from the Ministry of Health.

The app, called AC19, was created by the same developer that has made clones of Telegram in the past.

The app is thought to have collected citizens' live location that it may have shared with the regime to track users' movement.

> "Of course, the app couldn't tell citizens if they had coronavirus. But what it could do is hoover up huge amounts of data on citizens, including names, addresses, dates of birth, and even track people's location in real time." VICE

The following week, the app was removed from Google's Play Store.

Singapore – 01/03/20

At the end of February, Singapore's Ministry of Health made information about victims of the virus available to the public. Following this, a developer turned the information into an interactive map so that citizens' could track the location of those infected.

The map quickly went viral, raising fears that it could lead to discrimination, stigmatisation and gross digital privacy violations.

> "We must demand more from authorities as the role of big data and technology in humanitarian response matures." Access Now

Taiwan – 18/02/20

According to ABC News, Taiwan's government granted all medical facilities access to patients' travel histories by combining data from the National Health Insurance Administration and Immigration Agency on February 18.

The report also suggests that those required to self-quarantine were "monitored through their cellphones."

The cabinet spokeswoman told The Guardian that the government "are not using advanced surveillance technology. It's simply tracking based on their phone's sim cards and their nearby base stations."

The country's response to the virus has been lauded by many, although concerns regarding the high degree of surveillance remain in some quarters.

Netanyahu referenced Taiwan's use of accessing mobile phone data in his address to the nation that outlined Israel's more draconian approach.

Physical Surveillance

In an attempt to slow the spread of COVID-19, governments around the world are also adopting increasingly extensive physical surveillance measures.

These include the deployment of facial recognition cameras equipped with heat sensors, surveillance drones used to monitor citizens' movements, and extensive CCTV networks in a bid to help enforce curfews.

Bahrain – 08/04/20

According to an article in Mobi Health Matters, "The Kingdom of Bahrain is keeping track of its active cases of COVID-19 via electronic bracelets."

The bracelets are connected to a contact tracing app via Bluetooth and are used to ensure infected citizens remain quarantined.

According to the article, "violators will face legal penalties, potentially being sentenced to imprisonment for a period of not less than three months."

India – 06/04/20

Live Mint reported on April 6 that "police forces are increasingly turning to drones or unmanned aerial vehicles (UAVs) to surveil populations and prevent the buildup of

crowds during the three-week lockdown."

The article continues, "In the national capital, police now rely on drones as a key surveillance instrument to keep tabs on people's movement during the lockdown."

USA – 06/04/20

According to the Associated Press, authorities in West Virginia approved the use of ankle monitors to track citizens that test positive for COVID-19 but refuse to quarantine on 6 March.

Australia – 30/03/20

On March 30, Australia's 9 News reported that the West Australian police force are to begin using drones to help enforce the lockdown measures.

According to the article: "Drones fitted with flashing police lights and sirens will be used to patrol beaches, parks and other areas, and will be able to deliver warnings to people disrespecting social distancing rules."

USA – 27/03/20

According to a tweet from Spectrum News NY1 on March 27, the NYPD have been using aerial footage to help enforce public gathering restrictions.

From the video, it appears helicopters, rather than drones, are being used.

United Kingdom 26/03/20

On March 26, Derbyshire Police uploaded a video to Twitter that showed the use of drones to monitor visitors to the Peak District, a national park in the UK.

The police force are also likely to have used Automatic Number Plate Recognition (ANPR) technologies to track the visitors. According to a following tweet: "Some number plates were coming back to keepers in #Sheffield, so we know that people are travelling to visit these areas."

In a later tweet, the police force said: “We understand that people will have differing views about this post, however, we will not be apologetic for using any legal and appropriate methods to keep people safe.”

Belgium – 21/03/20

A tweet by Raphael-Antonis Stylianou, the EU Commission’s Online Communications Officer, appeared to show the use surveillance drones in Brussels on March 21.

The video shows a drone emitting a warning through its speakers, urging citizens to respect social distancing measures.

Raphael-Antonis Stylianou
@Stylianou_EU

In today's episode of #BlackMirror, the Belgian Police @zpz_polbru flying a #drone in Parc du Cinquantenaire in #Brussels. The drone emits warnings through speakers, asking citizens to respect social distancing measures.
So, this just happened 🤦‍♂️

1,205 5:45 PM - Mar 21, 2020 · Jubelpark / Parc du Cinquantenaire

762 people are talking about this

Spain- 14/03/20

On March 14, Madrid's Police Force tweeted: "We will not hesitate to use all the means that we have to ensure your security."

The tweet included videos of new surveillance drones that the police force are being used to enforce the ongoing lockdown.

The drones are equipped with speakers and have been filmed urging citizens to stay at home.

As Charlie Wood has written for Business Insider: "Spain's tactics bear some resemblance to reported surveillance tactics used by China."

Russia – 21/02/20

On Friday, 21 February, Reuters reported that Moscow's mayor had announced the use of facial recognition to help ensure people remained at home.

According to the article, the mayor wrote on his website: "Compliance with the regime is constantly monitored, including with the help of facial recognition systems and other technical measures."

According to one report, over 200 people have been found to be disobeying the self-quarantine orders by the city's 'Safe City' surveillance system.

China – 20/01/20

Since the outbreak of the virus, the Chinese regime has used a host of surveillance measures to try and stem the spread of the disease.

This has included the use of drones, facial recognition cameras and mobile phone monitoring.

Two of the country's largest state-owned telecommunication operators, China Unicom and China Telecom, asked citizens in Wuhan to provide the personal information in order to link them to their devices and allow more effective monitoring.

It is hardly surprising that China, the country with the most sophisticated surveillance infrastructure in the world, would deploy these measures in response to the outbreak.

However, many are concerned these new measures will become the new normal and remain in place after the virus subsides.

As Wang Aizhong, an activist based in Guangzhou, told The Guardian:

> "This epidemic undoubtedly provides more reason for the government to surveil the public. I don't think authorities will rule out keeping this up after the outbreak."

Censorship

Since the outbreak of COVID-19 there has been a rapid acceleration in the spread of mis- and disinformation.

According to a recent document seen by Reuters, for example, Russian media outlets have been involved in a "significant disinformation campaign" in an attempt to worsen the impact of the virus and create confusion in the West.

To control this, governments and social media platforms have sought to stringently regulate online content and promote official facts and figures from international health organisations.

However, several governments have also co-opted the rise of mis/disinformation to justifying censorship practices which seek to silence critics and control the flow of information.

Turkmenistan 31/03/20

According to a report by Reporters Without Borders, authorities in Turkmenistan banned the use of the word 'coronavirus' in public at the end of March.

Jeanne Cavelier, the head of RSF's Eastern Europe and Central Asia desk, said: "This denial of information not only endangers the Turkmen citizens most at risk but also

reinforces the authoritarianism imposed by President Gurbanguly Berdymukhammedov."

Iran – 25/03/20

On March 25, Voice of America reported: "As coronavirus spreads in Iran, authorities have moved swiftly and aggressively to contain independent reporting about it by harassing, detaining and censoring journalists and social media users."

According to the article, "Tehran has questioned or detained journalists who contradicted or questioned official reports, warned that those publishing statistics other than government figures would be arrested, and issued censorship orders to news outlets."

Thailand – 25/03/20

Human Rights Watch reported on March 25 that Thai officials had been "using "anti-fake news" laws to prosecute people critical of the government's response to the COVID-19 pandemic."

According to the press release, Prime Minister Prayut introduced a list of new prohibitions on March 25, which included: "Reporting or spreading of information regarding COVID-19 which is untrue and may cause public fear, as well as deliberate distortion of information which causes misunderstanding and hence affects peace and order, or good moral of people."

Russia – 25/03/20

On March 25, the Committee to Protect Journalists released a statement calling on Russian authorities to stop censoring media outlets reporting on the virus.

According to group's statement: "Russia's media regulator, Roskomnadzor, had ordered articles to be removed from their websites and social media and threatened them with fines."

Cambodia – 24/03/20

Since the beginning of January, Human Rights Watch have documented 17 social media users that have been arrested for sharing information about COVID-19 in Cambodia.

According to the human rights watchdog, this included a 14-year-old girl who was arrested and questioned because she "expressed fears on social media about rumors of positive COVID-19 cases at her school and in her province."

Niger – 24/03/20

According to a report by the Committee to Protect Journalists on March 24, authorities in Niger had arrested a prominent journalist due to his coverage of the virus.

Angela Quintal, the CPJ's Africa programme coordinator, said: "Kaka Touda Mamane Goni and all other journalists in Niger should be free to cover the ongoing COVID-19 outbreak without fearing that they will be thrown in jail. Niger authorities should release Kaka Touda immediately, ensure he is given proper medical care, and drop their case against him."

Uganda – 23/03/20

According to digital rights advocacy organisation, Unwanted Witness, a social media user was was arrested in Uganda on March 23 for posting content related to COVID-19.

According to the group's report: "After registering a COVID- 19 case in Uganda, the country's telecommunications regulator, Uganda Communications Commission (UCC) has tightened social media censorship."

Hong Kong – 19/03/20

On March 19, Radio Television Hong Kong, the public broadcasting service of Hong Kong, reported that: "Two prominent University of Hong Kong microbiologists [...] retracted a column they co-wrote sharply criticising the continuing practice on the mainland of consuming wild game."

Kenneth Roth, the Executive Director of Human Rights Watch, tweeted in response: "Beijing's censorship extends to Hong Kong, as scientists retract an article that had criticized the Chinese government's refusal after the 2003 SARS outbreak to close game meat markets in which SARS and now COVID-19 are believed to have jumped to humans."

Egypt – 18/03/20

On March 18, Al Jazeera reported that "Egypt has revoked the press credentials of a British journalist with the UK's Guardian newspaper, and censured the New York Times Cairo bureau chief over 'bad faith' reporting on the country's coronavirus cases."

The move followed a story by Ruth Michaelson in the Guardian that suggested that the number of coronavirus cases in the country were likely higher than official reporting had suggested.

Kenya – 16/03/20

According to a story by the Daily Nation, an independent Kenyan newspaper, "Detectives [...] arrested a man for allegedly publishing misleading and alarming information about the Covid-19 (novel coronavirus) outbreak" on March 16.

It was reported that the individual is to be charged under Section 23 of Kenya's Computer Misuse and Cybercrimes Act of 2018.

The act has been criticised by a variety of civil society organisations, including Article 19, which said the act "lacks critical amendments [...] needed to protect the right to freedom of expression and information online in Kenya."

Singapore – 16/03/20

On March 16, the Washington Post reported that Facebook had been ordered to block local access to a popular Facebook page by Singapore's government.

The page, States Times Review, was swiftly removed by the social media giant as deciding not to comply would mean the company could face a fine of over $14,000 a day.

Authorities claimed that the page was disseminating false information regarding the coronavirus outbreak.

The page was operated by Alex Tan, a prominent Singaporean dissident who is renowned for his outspoken and critical articles.

Facebook said that it was "deeply concerned" about the government's decision to block access to the page.

Iran – 02/03/20

Iranian authorities blocked access to the Farsi language edition of Wikipedia on Monday, 2 March 2020.

According to Netblocks, the restrictions lasted for 24 hours amid "international criticism as well as misinformation over the state's handling of the coronavirus epidemic."

This is not the first time Iranian authorities have looked to restrict citizens' ability to access the online encyclopedia.

China – 31/12/19

According to a recent report by Citizen Lab, live-streaming platform, YY, began censoring words related to the outbreak on December 31,2019.

WeChat also quickly began censoring COVID-19 related content and expanded its efforts in February.

According to Citizen Lab: "Many of the censorship rules are broad and effectively block messages that include names for the virus or sources for information about it. Such rules may restrict vital communication related to disease information and prevention."

It is a view shared by the international human rights advocacy organisation, Human Rights Watch.

According to their latest report: "China's government initially withheld basic information about the coronavirus from the public, underreported cases of infection, downplayed the severity of the infection, and dismissed the likelihood of transmission between humans."

Internet Shutdowns

Access Now have written: "As the world deals with the spread of COVID-19 ("coronavirus"), reliable, correct information is one of the most important tools people have to protect themselves."

Despite the urgent need for the free flow of critical health information, however, four governments continue to restrict internet access in their county.

The impact of these restrictions could be hugely damaging, and undoubtedly puts vulnerable communities further at risk.

Ethiopia

Since January, the Ethiopian government — which has a long history of internet shutdowns — has restricted access in the Oromia region.

The restrictions were implemented amid violent conflict between armed groups and the government.

Since the country has confirmed several cases of COVID-19, the government has been spreading vital health information online.

As Access Now made clear, "Publishing information online and via the media makes sense, but the government is also denying access to this valuable information to the population affected by internet shutdowns, and as a result, that population may further escalate the spread of the virus.

On March 31, the Ethiopian government vowed to end the internet shutdown in the region and on April 02, Telecom Paper reported that "Internet and voice services have been restored in several areas of the Oromo region in Ethiopia."

However, it remains unclear whether or not it has been restored across the entire region.

India

In the Jammu and Kashmir regions of India, citizens are only able to access 2G connections. Restrictions began in August 2019 and, although connections have been restored, the slow speeds of 2G dramatically limits the flow of critical health information.

It also limits citizens' ability to communicate with their families during a period of volatility and extreme apprehension.

Bangladesh

The Bangladeshi government has shutdown mobile internet connections and prevented refugees from using SIM cards in its Rohingya refugee camps since 2019.

According to Human Rights Watch, these restrictions “disrupt critical humanitarian and emergency services

By restricting internet access in refugee camps, the Bangladeshi authorities are putting an already vulnerable group at greater risk.

Myanmar

The internet has been blocked in nine townships of Rakhine and Chin states since 2019 amid the violent armed conflict that continues today.

In a press release from last year, the United Nations wrote: “Uninterrupted availability of the internet is indispensable and mobile internet services are a key enabler of the humanitarian and development work of the United Nations in Myanmar.”

By continuing internet restrictions in the country, many of the most vulnerable will be unable to access critical information regarding the virus.

The internet shutdown in Myanmar is one of the longest in the world.

Guinea – 21/03/20 – 23/03/20

Social media restrictions were implemented for 36 hours in Guinea as the country went to the polls to vote in a referendum that opposition groups fear could allow the president, Alpha Condé, to govern for an additional 12 years.

According to Netblocks, “Twitter, Facebook and Instagram were blocked while WhatApp servers were partially restricted. The restrictions continued through election day, 22 March, limiting global visibility into events as they took place.”

Previous Updates

31/03/20 Update

In March, we documented **21 new digital tracking measures** implemented around the world in response to COVID-19.

These varied from targeted contact tracing apps, to the large-scale acquisition of aggregated and anonymised location data.

We also documented 11 new reports of COVID-19-related censorship and 6 new physical surveillance initiatives in March alone.

> As the virus continues to spread around the world, so too do sophisticated surveillance measures and restrictive censorship practices.

26/03/20 Update

Since Thursday 19 March, we have documented **14 new measures** implemented in response to the spread of the virus.

This includes nine new digital tracking measures, four reports of censorship, and one new physical surveillance initiative.

> In the past week we have witnessed a 90% growth in the number of countries implementing digital tracking measures and a 100% increase in reports of censorship.

From new contact tracing efforts in Russia, to increased social media censorship in Uganda, governments around the world are increasingly looking to technology in an attempt to control the pandemic.

There have also been multiple reports of plans to begin digital tracking measures in Canada and the US, although they are yet to be implemented.

There have also been several significant reports of international plans to track mobile phone users.

According to a recent story by Stephanie Kirchgaessner in the Guardian, for example: "The mobile phone industry has explored the creation of a global data-sharing system that could track individuals around the world, as part of an effort to curb the spread of Covid-19."

To date, European countries have implemented the most digital tracking measures, while countries in Asia have been accused of censoring digital content the most.

Supporting Documents & Additional Resources

For more updates on proposed and confirmed developments from around the world, follow Privacy International's live tracker, Tracking the Global Response to COVID-19, and this document created by Dr. Andrew Dwyer.

About Top10PVN

Top10VPN.com is an internet research firm and leading VPN review website. We recommend the best VPN services to help protect consumers' privacy online. We also aim to educate the general public about digital privacy and cybersecurity risks through our free online resources and research.

For more original security and privacy research, check out our The Global Cost of Internet Shutdowns in 2019, Free VPN App Investigation, or Free VPN Risk Index (Android).

Related

US Trade Show to Promote Controversial Chinese Companies

5 Mar 2020 10:30 GMT

Home Office to Host Controversial Surveillance Companies

17 Feb 2020 10:00 GMT