

# FREEDOM ON THE NET 2019

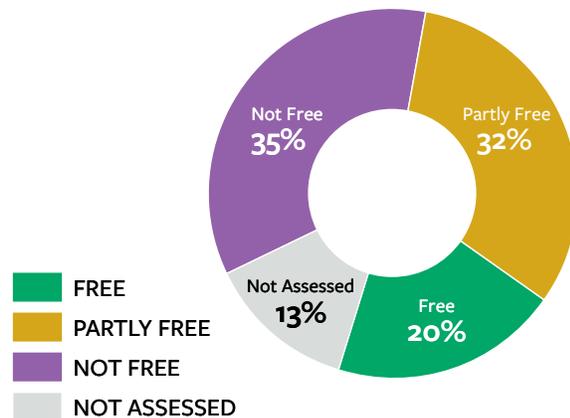
## The Crisis of Social Media

### Key Global Findings

- Declines outnumber gains for the ninth consecutive year.** Since June 2018, 33 of the 65 countries assessed in *Freedom on the Net* experienced a deterioration in internet freedom. The biggest score declines took place in Sudan and Kazakhstan, followed by Brazil, Bangladesh, and Zimbabwe.
- Improvements measured in 16 countries,** with Ethiopia recording the largest gains.
- Internet freedom declines in the United States, yet remains Free.** US law enforcement and immigration agencies increasingly monitored social media and conducted warrantless searches of travelers' electronic devices, at times monitoring constitutionally protected activities. Disinformation was again prevalent around major political events, spread increasingly by domestic actors.
- China is the world's worst abuser of internet freedom for the fourth consecutive year.** Censorship reached unprecedented extremes as the government enhanced its information controls ahead of the 30th anniversary of the Tiananmen Square massacre and in the face of persistent antigovernment protests in Hong Kong.
- Free expression is under assault.** A record high of 47 out of 65 countries featured arrests of users for political, social, or religious speech. Individuals endured physical violence in retribution for their online activities in at least 31 countries.
- Governments around the world are increasingly using social media to manipulate elections and monitor their citizens,** tilting the technology toward digital authoritarianism.

### GLOBAL INTERNET POPULATION BY 2019 FOTN STATUS

*Freedom on the Net* assesses 87 percent of the world's internet user population.

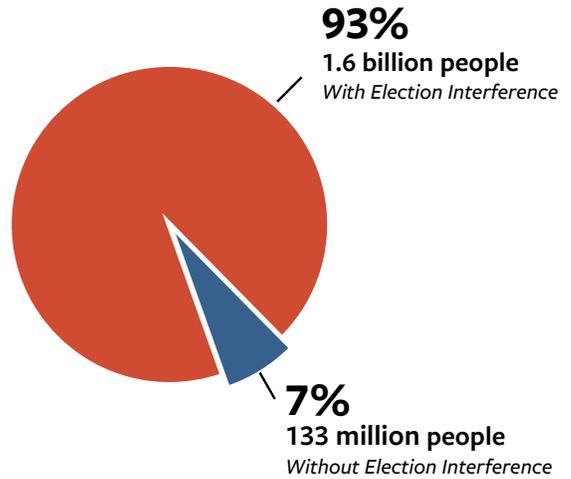


# Digital Election Interference

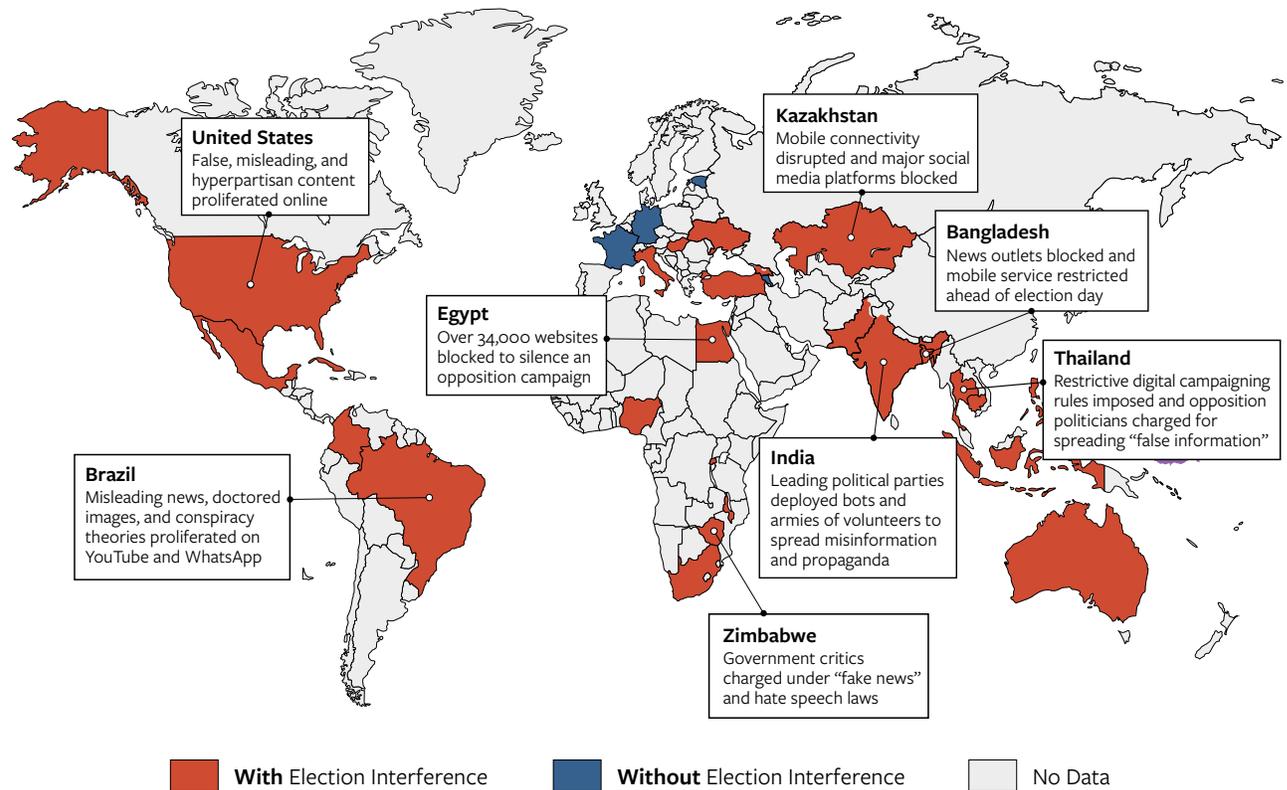
Internet freedom restrictions escalate before and during crucial votes, as evidenced in 2019. Shaping the flow of information online is now an essential strategy of those seeking to disrupt the democratic transfer of power.

- Cross-border influence operations are an increasingly common problem. China, Iran, Saudi Arabia, and a growing list of other countries have expanded their efforts to manipulate the online environment and influence foreign political outcomes over the past year.
- In a majority of countries evaluated, however, it was **domestic actors** who abused information technology to subvert the electoral process.

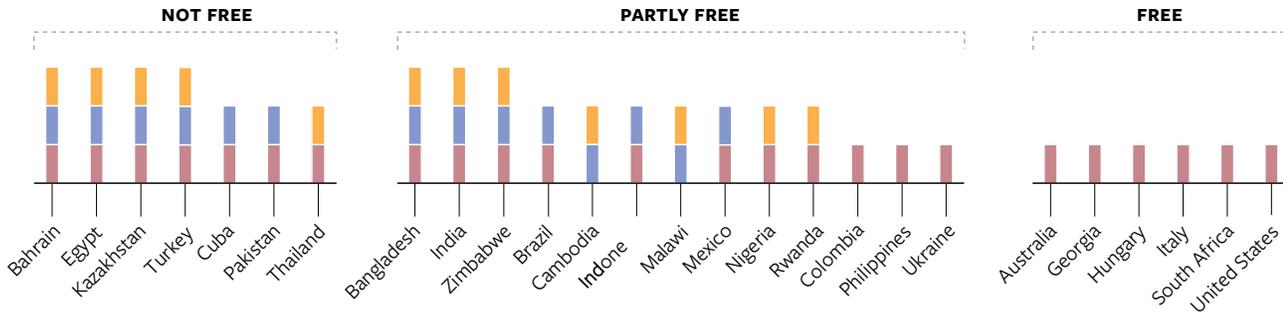
*In countries that held elections or referendums, an alarming number of internet users were exposed to informational, technical, or legal interference by domestic actors.*



*Domestic actors interfered online in 26 of 30 countries that held elections or referendums over the past year.*



## Key Tactics of Digital Election Interference



### Informational tactics

The coordinated use of hyperpartisan commentators, bots, group admins, or news sites to disseminate false or misleading content, often with the backing of the state or a political party apparatus.

### Technical tactics

Intentional restrictions on connectivity; blocking of social media platforms and websites; and cyberattacks from suspected domestic actors on political websites or social media accounts.

### Legal tactics

Arrests of individuals for online political expression, as well as the establishment of new laws and regulations that criminalize online speech.

- In **26 out of the 30 countries** that held elections or referendums over the past year, Freedom House found at least one of three distinct forms of digital election interference: informational measures; technical measures; and legal measures.
- **Informational measures:** State and nonstate actors distorted the online landscape during elections in 24 countries over the past year, making it by far the most popular tactic. Often working in tandem with government-friendly media personalities and business magnates, semiautonomous online mobs transmitted conspiracy theories, inflammatory views, and misleading memes from marginal echo chambers to the political mainstream.
- **Technical measures:** Technical measures played a role in the elections of at least 14 countries during the coverage period.
- **Legal measures:** In 12 countries, authorities employed legal measures to control online speech during election periods. One of the most common charges was defaming public officials.

## Social Media Surveillance

Governments are increasingly purchasing sophisticated technology to monitor their citizens' behavior on social media. Advances in artificial intelligence have made these tools more affordable for a much broader range of states.

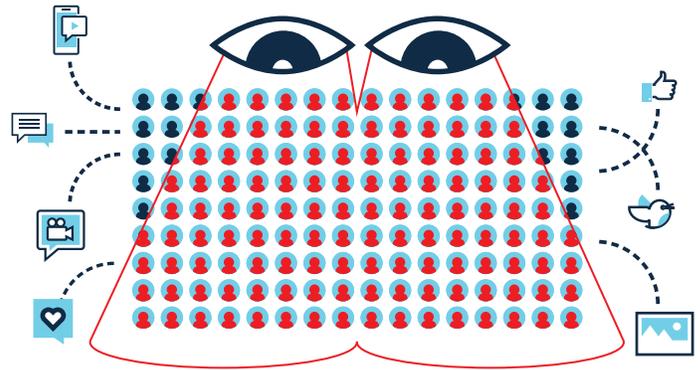
Sophisticated monitoring systems can quickly map users' relationships through link analysis; assign a meaning or attitude to their social media posts using natural-language processing and sentiment analysis; and infer their past, present, or future locations.

- At least **40 of the 65 countries** covered by *Freedom on the Net* have instituted advanced social media monitoring programs.
- **China** is a leader in developing, employing, and exporting social media surveillance tools. **Nigeria, Russia, Pakistan, Kazakhstan, Kenya,** and the **Philippines** are among the other countries monitoring their citizens' social media behavior.

## The potential for abuse presented by advanced social media surveillance is staggering.

- Federal and local agencies within the **United States** are monitoring social media, with limited oversight and transparency. In some worrisome cases, such monitoring targeted constitutionally protected activities such as peaceful protests and newsgathering.
- There is little if any public evidence that such technology is more effective than less-invasive alternatives for ensuring national security and combating serious crimes.
- Social media activity such as original content, likes, or shares—particularly speech that is rendered in slang or languages other than English—is susceptible to misinterpretation and misclassification. Research has estimated the accuracy rates of natural-language processing tools at 70 to 80 percent.

40 of the 65 countries covered by *Freedom on the Net* have instituted advanced social media surveillance programs. That means 89% of internet users—or nearly 3 billion people—are being monitored.



Authorities can collect and analyze details about personal relationships, spiritual beliefs, and sexual preferences, and share them with third parties.

Human and algorithmic bias perpetuates harmful and incorrect stereotypes, disproportionately impacting marginalized communities.

Immigration officials can deny individuals entry based on their political, social, or religious views expressed on social media, or that of their friends and family.

People refrain from speaking out on political, social, and religious issues when they fear their speech could be recorded and potentially used against them.

Individuals become less likely to join organizations and groups if authorities can monitor their memberships and activities.

Authorities can disrupt nonviolent demonstrations before they begin, and track the names of individuals in attendance.

Monitoring eschews democratic legal standards of “reasonable suspicion” and “probable cause,” and instead treats everyone as a suspect of wrongdoing.

**VIOLATES PRIVACY**

**ENABLES DISCRIMINATION**

**THREATENS MIGRANTS’ RIGHTS**

**RESTRICTS FREE EXPRESSION**

**DISCOURAGES FREEDOM OF ASSOCIATION**

**DISRUPTS FREEDOM OF ASSEMBLY**

**UNDERMINES DUE PROCESS**

Democracy requires vibrant public spaces free from constant surveillance.



## Biggest Declines in Net Freedom

- **Sudan:** Amid nationwide protests that led to the ouster of President Omar al-Bashir, authorities blocked social media platforms and suspended the constitution.
- **Kazakhstan:** After the unexpected resignation of longtime president Nursultan Nazarbayev, authorities temporarily disrupted internet connectivity and blocked over a dozen local and international news websites.
- **Brazil:** The victory of Jair Bolsonaro in the October 2018 presidential election proved a watershed moment for digital election interference in the country, as disinformation proliferated across WhatsApp.

### Worst of the Worst

Country	Score
China	10
Iran	15
Syria	17
Cuba	22
Vietnam	24

### Best of the Best

Country	Score
Iceland	95
Estonia	94
Canada	87
Germany	80
United States	77

## Recommendations

*Internet freedom rests on our ability to fix social media.*

### Securing Elections

- **Improve transparency and oversight of online political advertisements** through legislation, such as the Honest Ads Act (S.1356/H.R.2592), that applies disclosure requirements to campaign advertising and requires large digital platforms to maintain a public file of all electioneering communications.
- **Address the use of bots in social media manipulation.** The Bot Disclosure and Accountability Act (S.2125) would authorize the Federal Trade Commission to require the conspicuous and public disclosure of bots intended to replicate human activity.
- **Protect elections from cyberattacks with paper ballots to ensure a verifiable paper trail and with election audits.** For example, the Protecting American Votes and Election Act (S.1472/H.R.2754) would mandate paper ballots and audits in federal elections, and provide funding for states to purchase new ballot-scanning machines.

### Preventing Abusive Social Media Surveillance

- **Strictly regulate the use of social media surveillance tools and the collection of social media information by government agencies and law enforcement.** Authorities should not proactively monitor social media for peaceful protests, nor should they conduct blanket reviews of content for immigration or visa evaluations.
- **Enact robust data privacy legislation.** Authorities should have the ability to access individual data only in limited circumstances as prescribed by law and subject to judicial authorization, and only within a specific time frame. In the United States, policymakers should pass a federal electronic privacy law that harmonizes rules among 50 states.
- **Restrict the export of sophisticated monitoring tools.** The United States is undergoing an interagency rulemaking process to determine which emerging dual-use technologies should be subject to export controls. Any final rule issued should ensure that technologies enabling monitoring, surveillance, and the interception or collection of information

and communications are included on the Commerce Control List and their sale be restricted to countries ranked Partly Free or Not Free by any Freedom House publication.

- **Require businesses exporting dual-use technologies to report annually on the impacts of their exports,** and identify where such technologies have been exported and any human rights concerns.

### Protecting Internet Freedom

- **Ensure that all internet-related laws and practices adhere to international human rights law and standards,** and establish periodic reviews to assess whether laws and practices do so.
- **Preserve broad protections against intermediary liability and focus new regulations on conduct, not content.** Companies should continue to benefit from safe harbor protections for most user-generated and third-party content appearing on their platforms, a principle that has allowed for a historic blossoming in artistic expression, economic activity, and social campaigning.



### GLOBAL INTERNET USER STATS

Over **3.8 billion** people have access to the internet.

According to Freedom House estimates:

**71%** live in countries where individuals were arrested or imprisoned for posting content on political, social, or religious issues.

**65%** live in countries where individuals have been attacked or killed for their online activities since June 2018.

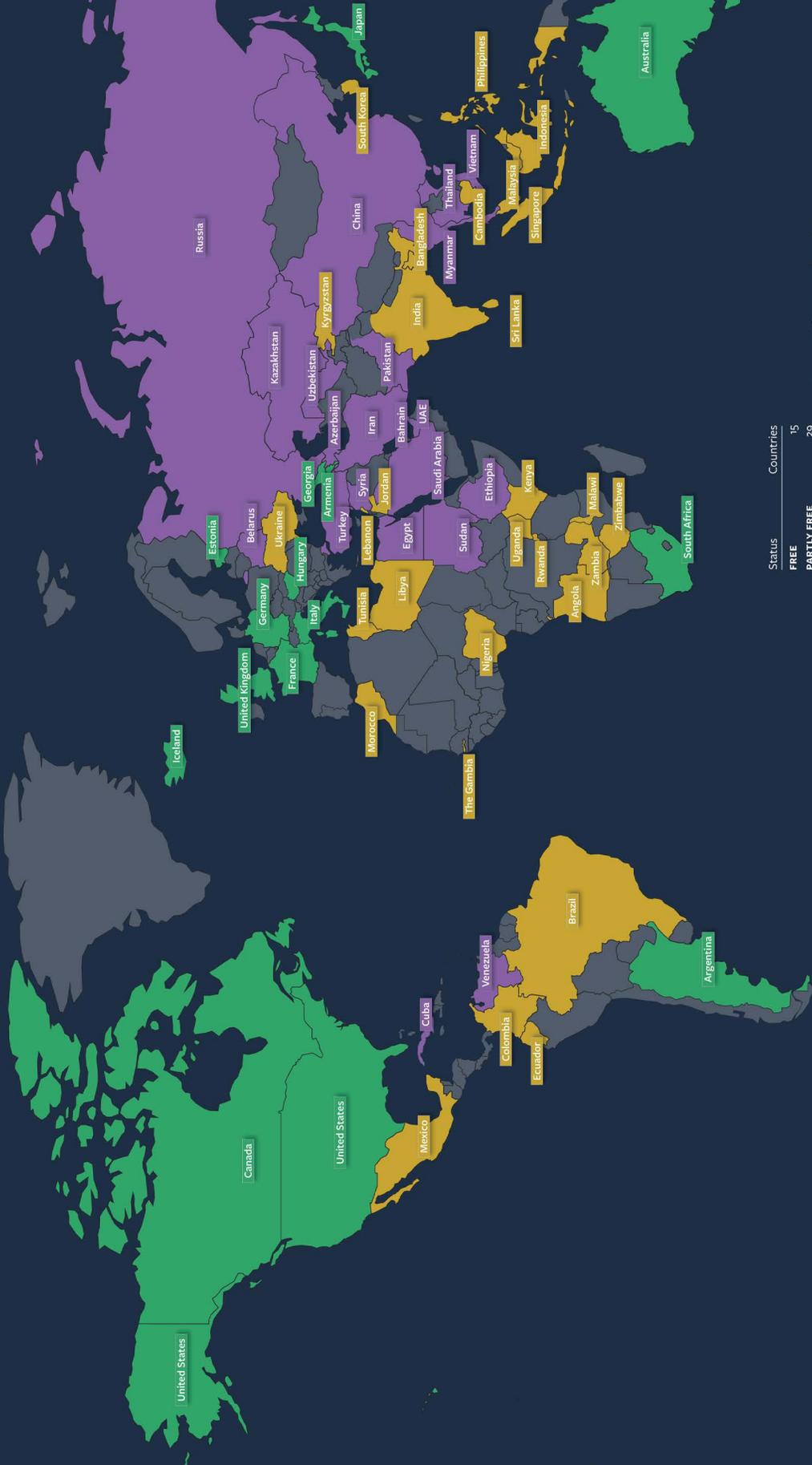
**59%** live in countries where authorities deployed progovernment commentators to manipulate online discussions.

**56%** live in countries where political, social, or religious content was blocked online.

**46%** live in countries where authorities disconnected internet or mobile networks, often for political reasons.

**46%** live in countries where access to social media platforms was temporarily or permanently restricted.

# FREEDOM ON THE NET 2019



Status	Countries
FREE	15
PARTLY FREE	29
NOT FREE	21
<b>Total</b>	<b>65</b>

For more information about the report's geographical coverage, visit [freedomofthenet.org](http://freedomofthenet.org).