Skip to main content

Freedom House

- Freedom in the World
- Freedom of the Press
- Freedom on the Net
- Nations in Transit
- Special Reports

Freedom on the Net

2016 ▾

Go

Freedom on the Net 2016

Freedom on the Net 2016

Silencing the Messenger: Communication Apps Under Pressure

Free
Partly Free
Not Free

Countries not assessed

= Score improvement, = Score decline

Free
Partly Free
Not Free
Countries not assessed

= Score improvement, = Score decline

Report Navigation

- Silencing the Messenger:
  Communication Apps Under Pressure
- 2016 Country Scores
- Key Internet Controls by Country
- Methodology
- About *Freedom on the Net*

Country Reports

- Select a Country Report - Angola Argentina Armenia Australia Azerbaijan Bahrain Bangladesh Belarus Brazil Cambodia Canada China Colombia Cuba Ecuador Egypt Estonia Ethiopia France Gambia, The Georgia Germany Hungary Iceland India Indonesia Iran Italy Japan Jordan Kazakhstan Kenya Kyrgyzstan Lebanon Libya Malawi Malaysia Mexico Morocco Myanmar Nigeria Pakistan Philippines Russia Rwanda Saudi Arabia Singapore South Africa South Korea Sri Lanka Sudan Syria Thailand Tunisia Turkey Uganda Ukraine United Arab Emirates United Kingdom United States Uzbekistan Venezuela Vietnam Zambia Zimbabwe

Downloads

- Report PDF
- Report + 65 Country Reports
- Report Graphics

Key Findings

- Internet freedom around the world declined in 2016 for the sixth consecutive year.
- Two-thirds of all internet users — 67 percent — live in countries where criticism of the government, military, or ruling family are subject to censorship.
- Social media users face unprecedented penalties, as authorities in 38 countries made arrests based on social media posts over the past year. Globally, 27 percent of all internet users live in countries where people have been arrested for publishing, sharing, or merely "liking" content on Facebook.
- Governments are increasingly going after messaging apps like WhatsApp and Telegram, which can spread information quickly and securely.

A Bahraini woman uses a mobile phone to take photos during clashes with riot police in Sitra, south of the capital Manama. Getty Images.

by Sanja Kelly, Mai Truong, Adrian Shahbaz, and Madeline Earp

Internet freedom has declined for the sixth consecutive year, with more governments than ever before targeting social media and communication apps as a means of halting the rapid dissemination of information, particularly during anti-government protests.

Public-facing social media platforms like Facebook and Twitter have been subject to growing censorship for several years, but in a new trend, governments increasingly target voice communication and messaging apps such as WhatsApp and Telegram. These services are able to spread information and connect users quickly and securely, making it more difficult for authorities to control the information landscape or conduct surveillance.

Freedom on the Net 2016 Overall Scores

Countries not assessed
0-10
11-20
21-30
31-40
41-50
51-60
61-70
71-80
81-90

Freedom on the Net Score: 0=Most Free, 100=Less Free

Internet freedom has declined for the sixth consecutive year, with more governments than ever before targeting social media and communication apps as a means of halting the rapid dissemination of information, particularly during anti-government protests.

The increased controls show the importance of social media and online communication for advancing political freedom and social justice. It is no coincidence that the tools at the center of the current crackdown have been widely used to hold governments accountable and facilitate uncensored conversations. Authorities in several countries have even resorted to shutting down all internet access at politically contentious times, solely to prevent users from disseminating information through social media and communication apps, with untold social, commercial, and humanitarian consequences.

Some communication apps face restrictions due to their encryption features, which make it extremely difficult for authorities to obtain user data, even for the legitimate purposes of law enforcement and national security. Online voice and video calling apps like Skype have also come under pressure for more mundane reasons. They are now restricted in several countries to protect the revenue of national telecommunications firms, as users were turning to the new services instead of making calls through fixed-line or mobile telephony.

Other key trends

Social media users face unprecedented penalties: In addition to restricting access to social media and communication apps, state authorities more frequently imprison users for their posts and the content of their messages, creating a chilling effect among others who write on controversial topics. Users in some countries were put behind bars for simply “liking” offending material on Facebook, or for not denouncing critical messages sent to them by others. Offenses that led to arrests ranged from mocking the king's pet dog in Thailand to "spreading atheism" in Saudi Arabia. The number of countries where such arrests occur has increased by over 50 percent since 2013.

Governments censor more diverse content: Governments have expanded censorship to cover a growing diversity of topics and online activities. Sites and pages through which people initiate digital petitions or calls for protests were censored in more countries than before, as were websites and online news outlets that promote the views of political opposition groups. Content and websites dealing with LGBTI (lesbian, gay, bisexual, transgender, and intersex) issues were also increasingly blocked or taken down on moral grounds. Censorship of images—as opposed to the written word—has intensified, likely due to the ease with which users can now share them, and the fact that they often serve as compelling evidence of official wrongdoing.

Security measures threaten free speech and privacy: In an effort to boost their national security and law enforcement powers, a number of governments have passed new laws that limit privacy and authorize broad surveillance. This trend was present in both democratic and nondemocratic countries, and often led to political debates about the extent to which governments should have backdoor access to encrypted communications. The most worrisome examples, however, were observed in authoritarian countries, where governments used antiterrorism laws to prosecute users for simply writing about democracy, religion, or human rights.

Online activism reaches new heights: The internet remained a key tool in the fight for better governance, human rights, and transparency. In over two-thirds of the countries in this study, internet-based activism has led to some sort of tangible outcome, from the defeat of a restrictive legislative proposal to the exposure of corruption through citizen journalism. During the year, for example, internet freedom activists in Nigeria helped thwart a bill that would have limited social media activity, while a WhatsApp group in Syria helped save innocent lives by warning civilians of impending air raids.

Tracking the global decline

Freedom on the Net is a comprehensive study of internet freedom in 65 countries around the globe, covering 88 percent of the world's internet users. It tracks improvements and declines in governments' policies and practices each year, and the countries included in the study are selected to represent diverse geographical regions and types of polity. This report, the seventh in its series, focuses on developments that occurred between June 2015 and May 2016, although some more recent events are included in individual country narratives. More than 70 researchers, nearly all based in the countries they analyzed, contributed to the project by examining laws and practices relevant to the internet, testing the accessibility of select websites, and interviewing a wide range of sources.

Of the 65 countries assessed, 34 have been on a negative trajectory since June 2015. The steepest declines were in Uganda, Bangladesh, Cambodia, Ecuador, and Libya. In Uganda, the government made a concerted effort to restrict internet freedom in the run-up to the presidential election and inauguration in the first half of 2016, blocking social media platforms and communication services such as Facebook, Twitter, and WhatsApp for several days. In Bangladesh, Islamist extremists claimed responsibility for the murders of a blogger and the founder of an LGBTI magazine with a community of online supporters. And Cambodia passed an overly broad telecommunications law that put the industry under government control, to the detriment of service providers and user privacy. Separately, Cambodian police arrested several people for their Facebook posts, including one about a border dispute with Vietnam.

China was the year’s worst abuser of internet freedom. The Chinese government’s crackdown on free expression under President Xi Jinping’s “information security” policy is taking its toll on the digital activists who have traditionally fought back against censorship and surveillance. Dozens of prosecutions related to online expression have increased self-censorship, as have legal restrictions introduced in 2015. A criminal law amendment added seven-year prison terms for spreading rumors on social media (a charge often used against those who criticize the authorities), while some users belonging to minority religious groups were imprisoned simply for watching religious videos on their mobile phones. The London-based magazine *Economist* and the Hong Kong–based *South China Morning Post* were newly blocked in mainland China, as were articles and commentaries about sensitive events including a deadly chemical blast in Tianjin in 2015.

Turkey and Brazil were downgraded in their internet freedom status. In Brazil, which slipped from Free to Partly Free, courts imposed temporary blocks on WhatsApp for its failure to turn over user data in criminal investigations, showing little respect for the principles of proportionality and necessity. Moreover, at least two bloggers were killed after reporting on local corruption. Turkey, whose internet freedom environment has been deteriorating for a number of years, dropped into the Not Free category amid multiple blockings of social media platforms and prosecutions of users, most often for offenses related to criticism of the authorities or religion. These restrictions continued to escalate following the failed coup in July 2016, in spite of the crucial role that social media and communication apps—most notably FaceTime—played in mobilizing citizens against the coup.

Just 14 countries registered overall improvements. In most cases, their gains were quite modest. Users in Zambia faced fewer restrictions on online content compared with the previous few years, when at least two critical news outlets were blocked. South Africa registered an improvement due to the success of online activists in using the internet to promote societal change and diversifying online content, rather than any positive government actions. Digital activism also flourished in Sri Lanka as censorship and rights violations continued to decline under President Maithripala Sirisena’s administration. And the United States registered a slight improvement to reflect the passage of the USA Freedom Act, which puts some limits on bulk collection of telecommunications metadata and establishes several other privacy protections.

Major developments

Social Media and Communication Tools Under Assault

In the past year, social media platforms, communication apps, and their users faced greater threats than ever before in an apparent backlash against growing citizen engagement, particularly during politically sensitive times. Of the 65 countries assessed, governments in 24 impeded access to social media and communication tools, up from 15 the previous year. Governments in 15 countries temporarily shut down access to the entire internet or mobile phone networks, sometimes solely to prevent users from disseminating information through social media. Meanwhile, the crackdown on users for their activities on social media or messaging apps reached new heights as arrests and punishments intensified.

New restrictions on messaging apps and internet-based calls

In a new development, the most routinely targeted tools this year were instant messaging and calling platforms, with restrictions often imposed during times of protests or due to national security concerns. Governments singled out these apps for blocking due to two important features: encryption, which protects the content of users' communications from interception, and text or audiovisual calling functions, which have eroded the business model and profit margins of traditional telecommunications companies.

Whatever the justification, restrictions on social media and internet-based communication tools threaten to infringe on users' fundamental right to access the internet. In a landmark resolution passed in July 2016, the UN Human Rights Council condemned state-sponsored disruptions to internet access and the free flow of information online.

WhatsApp faced the most restrictions, with 12 out of 65 countries blocking the entire service or disabling certain features, affecting millions of its one billion users worldwide. Telegram, Viber, Facebook Messenger, LINE, IMO, and Google Hangouts were also regularly blocked. Ten countries restricted access to platforms that enable voice and video calling over the internet, such as Skype and FaceTime.

Nearly ubiquitous among internet and mobile phone users, these communication platforms have become essential to the way we connect with the world. Incidents of blocking have had far-reaching effects, preventing family members from checking in during a crisis, activists from documenting police abuses during a protest, and individuals from communicating affordably with social and professional contacts abroad.

While all users are adversely affected by restrictions, the harm is often disproportionately felt by marginalized communities and minority groups, who are more likely to be cut off from critical information sources and the ability to advocate for their rights. In the United Arab Emirates (UAE), for example, where migrant workers and other noncitizens make up 88 percent of the population, blocks on communication tools have made it difficult for these individuals to organize or seek support from their home countries.

App blocking aimed at protests, expressions of dissent

Authoritarian regimes most frequently restricted communication apps to prevent or quell antigovernment protests, as they have become indispensable for sharing information on demonstrations and organizing participants in real time. In Ethiopia, ongoing protests that began in November 2015 in response to the government's marginalization of the Oromo people have been met with periodic blocks on services including WhatsApp, Facebook Messenger, and Twitter. In Bahrain, Telegram was blocked for several days around the anniversary of the February 14, 2011, "Day of Rage" protests, likely to quash any plans for renewed demonstrations.

In Bangladesh, the authorities ordered the blocking of platforms including Facebook Messenger, WhatsApp, and Viber to prevent potential protests following a Supreme Court ruling in November that upheld death sentences for two political leaders convicted of war crimes. The longest block lasted 22 days. In Uganda, officials directed internet service providers to block WhatsApp, Facebook, and Twitter for several days during the presidential election period in February 2016 and again in the run-up to the reelected incumbent's inauguration in May. In both instances, the unprecedented blocking worked to silence citizens' discontent with the president's 30-year grip on power and their efforts to report on the ruling party's notorious electoral intimidation tactics.

New security and encryption features also trigger blocking

Governments increasingly imposed restrictions on internet-based messaging and calling services due to their strong privacy and security features, which have attracted many users amid growing concerns about surveillance worldwide.

In many countries, individuals are using messaging apps as private social networks where they can enjoy greater freedom of expression than on more established, public-facing social networks such as Facebook and Twitter. New messaging and calling apps also provide greater anonymity than conventional voice and SMS services that can be tracked due to SIM-card registration requirements, and several offer end-to-end encryption that prevents wiretapping and interception.

Activists and human rights defenders in repressive countries protect their communications by convening on WhatsApp, Viber, and Telegram to share sensitive information, conduct advocacy campaigns, or organize protests. Journalists in Turkey, for example, have established new distribution networks for their reporting via group channels on WhatsApp to avert censorship.

The same security features that appeal to users of the new platforms have brought them into conflict with governments in both democratic and authoritarian countries. In Brazil in 2015 and 2016, regional courts ordered a block on WhatsApp three times after it failed to turn over encrypted communications to local authorities during criminal investigations. On all three occasions, WhatsApp's parent company, Facebook, insisted that it did not have access to the information in question, since WhatsApp does not store the content of users' communications. Nevertheless, the judges chose to penalize not just the company, but also Brazil's 100 million WhatsApp users.

Authoritarian regimes targeted Telegram for its "secret chat" mode, which allows messages to self-delete after a period of time. The platform was blocked in China after the authorities learned of its popularity among human rights lawyers, joining a long list of other international communication apps that are unavailable to Chinese users. State-run news outlets in the country accused Telegram of aiding activists in "attacks on the [Communist] Party and government." Iran also targeted Telegram, blocking it for a week in October 2015 when it refused to aid officials' surveillance and censorship efforts. In May 2016, Iran's Supreme Council on Cyberspace ordered Telegram to host all data on Iranian users inside the country or face blocking.

Market threats to national telecoms lead to backlash

Internet-based messaging and calling platforms faced increasing restrictions from governments seeking to protect their countries' major state-owned or private telecommunications companies. Given the rising popularity of new communication services over the past decade, telecoms in some markets have become concerned about the future economic viability of their traditional text and voice services, particularly when the new competitors are not subject to the same regulatory obligations and fees.

Typically free to download, messaging platforms such as WhatsApp, Telegram, and Facebook Messenger have proliferated in emerging markets, where the advent of low-cost, internet-enabled mobile devices and smartphones have made sending messages, photos, and even videos via online tools much more affordable than traditional SMS, for which telecom carriers charge a variable rate per message. Indeed, app-based mobile messaging has surpassed SMS texting worldwide since at least 2013.

Similarly, Voice over Internet Protocol (VoIP) and internet-based video calling services such as Skype, Google Hangouts, and Apple's FaceTime have significantly reduced the cost of real-time audio and visual communication for users, resulting in the decreased use of traditional phone services that charge by the minute. Though telecom companies still profit from the data used by internet-based platforms, continual improvements in network infrastructure have only made data plans cheaper, threatening to leave traditional voice and SMS services further behind.

One of the first market-related restrictions on internet-based communication services was imposed by the American telecommunications company AT&T in 2007, when it partnered with Apple to become the sole mobile provider for the first iPhone and subsequently banned VoIP applications that could make calls using a wireless data connection. Google's Voice app was consequently rejected by the iPhone's app store, and Skype developed a version of its platform that only allowed iPhone users to make calls when connected to a Wi-Fi network. Under pressure from the Federal Communications Commission (FCC), AT&T changed course in 2009, setting a positive precedent and providing users with more freedom to choose from a suite of services based on quality and affordability.

In the past year, restrictions to protect market interests escalated most prominently in the Middle East and North Africa. The UAE had been an early mover, requiring VoIP services to obtain a license to operate as a telecom provider and subsequently blocking both the voice and video calling features of Skype, WhatsApp, and Facebook Messenger in 2014, in an effort to protect the profits of state-owned telecom companies. Most recently, Snapchat's calling function was disabled in April 2016. While circumvention tools such as virtual private networks (VPNs) were widely used to bypass the blocks, the government cracked down in July 2016, adopting amendments to the Cybercrime Law that penalize the "illegal" use of VPNs with temporary imprisonment, fines of between US$136,000 and US$545,000, or both.

Morocco's telecommunications regulator issued a directive in January 2016 that suspended all internet calling services over mobile networks, citing previously unenforced licensing requirements under the 2004 telecommunications law. The order seemed heavily influenced by the UAE's Etisalat, which purchased a majority stake in Maroc Telecom, the country's largest operator, in 2014. In Egypt, where long-distance VoIP calls on Skype have been blocked since 2010, voice calling features on WhatsApp and Viber have reportedly been inaccessible since October 2015. The calling functions of popular platforms were also disabled in Saudi Arabia, while Apple has been forced to sell its iPhone in the kingdom without the built-in FaceTime app.

Pressure to regulate mobile communication services in the past year threatened to impede access to such platforms in other regions, particularly sub-Saharan Africa, where mobile internet use has been growing rapidly. In Kenya, Nigeria, South Africa, and Zimbabwe, private telecommunications companies lobbied governments to regulate internet-based messaging and voice calling platforms such as Skype and WhatsApp, citing concerns over their profits. Meanwhile, Ethiopia's single telecommunications provider, state-owned EthioTelecom, announced plans in April 2016 to introduce a new pricing scheme for mobile users of popular communication applications. Companies in the European Union (EU) pushed EU officials throughout 2016 to regulate new communication services, calling for a "level playing field" that subjects messaging and calling platforms to the same regulatory framework, licensing fees, and law enforcement access requirements as traditional telecoms.

Social media users face unprecedented penalties

While many governments attempted to restrict access to social media and communication platforms, far more turned to traditional law enforcement methods to punish and deter users. Since June 2015, police in a remarkable 38 countries arrested individuals for their activities on social media[ME6] , compared with 21 countries where people were arrested for content published on news sites or blogs. The rising penetration of social networks in repressive societies has enabled discussion and information sharing on issues that governments deem sensitive, resulting in arrests of journalists, politicians, activists, and ordinary citizens who may not be aware that they are crossing redlines.

A Turkish man was handed a one-year suspended sentence for this meme juxtaposing President Reçep Tayyip Erdogan and a character from the Lord of the Rings films. In determining whether or not the image insulted the president, the judge assembled a panel of film experts. Another user is facing up to two years in prison for reposting the same memes.

Dramatic sentences for social media 'crimes'

Social media users were prosecuted for a range of alleged crimes during the coverage period. Some supposed offenses were quite petty, illustrating both the sensitivity of some regimes and the broad discretion given to police and prosecutors under applicable laws. Lebanon's bureau of cybercrimes interrogated a Facebook user for criticizing a Lebanese singer, while soldiers in the UAE were arrested for disrespecting the army after they shared a video of themselves recreating a popular dance craze in their uniforms.

While severe punishments for online speech are not new, their application to social media activities that many people engage in daily was a cause for serious concern. In February 2016, a Saudi court sentenced an individual to 10 years in prison and 2,000 lashes for allegedly spreading atheism in 600 tweets. In the harshest examples of the coverage period, military courts in Thailand issued 60- and 56-year sentences in separate cases involving Facebook posts that were deemed critical of the monarchy in August 2015, though they were reduced to 30 and 28 years after the defendants pleaded guilty. While sentences like these may not cause people to stop using social media entirely, they are likely to encourage self-censorship on sensitive topics, robbing the technology of its potential for galvanizing social and political change.

Many detentions were justified under criminal laws penalizing defamation or insult, but they often aimed to suppress information in the public interest. In Morocco, YouTube footage of a man lifting asphalt barehanded from a local road led to his arrest for allegedly defaming the official responsible for the poor construction.

Users punished for their connections and readership

One goal of social media is to allow users to share content with a wide circle of connections. Police in some countries seem determined to undermine that goal, specifically pursuing individuals whose content goes viral. In Zimbabwe, Pastor Evan Mawarire was arrested in July 2016 after his YouTube videos criticizing the country's leadership sparked the #ThisFlag social media campaign and inspired nationwide protests. Elsewhere, charges often multiplied as content was passed along: In November 2015, 17 people in Hungary were charged with defamation for sharing a Facebook post that questioned the legitimacy of the mayor of Siófok's financial dealings.

In a disturbing development, defendants whose content failed to spread widely were nevertheless punished as a warning to others. In Russia, mechanical engineer Andrey Bubeyev was sentenced to two years in prison in May 2016 for reposting material that identified the Russian-occupied Crimean Peninsula as part of Ukraine on the social network VKontakte. He shared the information with just 12 contacts.

Authorities in other cases scoured social media for a pretext to charge specific individuals, or were so intent on suppressing certain content that identifying the correct defendant was of secondary importance. In Ethiopia, charges against an opposition politician and student protesters principally cited evidence gleaned from social media. Pseudonymous accounts offered limited protection and raised the risk of mistaken identity. A man in Uganda was charged on suspicion of operating the popular Facebook page Tom Voltaire Okwalinga, but he denied being responsible for the page, which frequently accused senior leaders of corruption and incompetence. Some people were held responsible for posts clearly made by others. At least three criminal charges were filed in India against the administrators of WhatsApp groups based on offensive or antireligious comments shared by other group members.

A number of users were apparently targeted only to punish their associates. In Thailand, Patnaree Chankij, the mother of an activist who opposes Thailand's military government, was charged with insulting the monarchy based on a private, one-word acknowledgement she sent in reply to a Facebook Messenger post from her son's friend; police said she failed to criticize or take action against the antiroyalist sentiment in the post, instead replying "yes" or "I see." Patnaree told journalists that the charge was in reprisal for her son's activities. In China, police detained the local relatives of at least three overseas journalists and bloggers who produce online content that the Chinese government perceives as critical.

Governments censor more diverse content

This year featured new trends in the type of content that attracted official censorship. Posts related to the LGBTI community, political opposition, digital activism, and satire resulted in blocking, takedowns, or arrests for the first time in many settings. Authorities also demonstrated an increasing wariness of the power of images on today's internet.

A longer roster of forbidden topics

Click on a region
to explore

Attempts to censor **LGBTI** content were observed in 18 countries, up from 14 in 2015, as more individuals and groups sought to use digital tools to connect and share resources, sometimes in defiance of local laws or religious beliefs. In July 2016, an LGBTI group reported that Azerbaijan's national domain-name registrar was declining to register website domains like lgbt.az. In Indonesia, the information ministry asked the LINE messaging platform to remove emojis with gay or lesbian themes from its online store. Also in 2016, South Korean regulators told the Naver web portal to exercise "restraint" after it linked to an online gay drama. At least 13 countries blocked content serving the LGBTI community on moral grounds, including Saudi Arabia and Sudan. Turkish authorities systematically blocked the most popular LGBTI websites over several weeks in mid-2015.

Content related to **political opposition** was subject to censorship in 26 countries, an increase from 23 in 2015. A court in Kazakhstan ordered an opposition-affiliated magazine to shutter its Facebook page along with its print edition in October 2015. In Bahrain, prosecutors questioned Sheikh Ali Salman, leader of the country's largest political organization, for allegedly tweeting about democracy, even though he was already imprisoned; police are now investigating who continues to operate the account.

Digital activism, including petitions, campaigns for social or political action, and protests, were subject to censorship in 20 countries in *Freedom on the Net*, up from 16 in 2015. Campaigns using smartphones or social media can appear dangerous because they are particularly effective at reaching young people. In The Gambia, a Facebook post calling on young people to join peaceful protests disappeared in April 2016 and was replaced with a warning to abide by the law; the protest organizer left the country, citing death threats. Because online mobilization amplifies discontent, authorities in many countries sought to shut it down even when the issues at stake were local. In Kazakhstan, two activists were arrested in May 2016 for planning on social media to attend land-reform protests scheduled to take place the next day.

Authorities in 26 of the 65 countries assessed, up from 23 in 2015, tried to suppress **satire**, which often skewered public officials. A poet in Myanmar was charged in November 2015 for posting a satirical poem on Facebook that described a newlywed's dismay at discovering a tattoo of the president on her husband's genitals.

Other topics that have long been subject to censorship remained in authorities' crosshairs this year:

- **Criticism of the authorities** was censored in 49 out of 65 countries, two more than in the previous year. In Cuba, for example, dissident or independent news sites that are perceived as critical—such as Cubanet, Penúltimos Días, Diario de Cuba, Cubaencuentro, Hablemos Press, and 14ymedio—are restricted at most internet access points.
- **Corruption allegations** were subject to censorship in 28 out of 65 countries Starting in July 2015, the Malaysian government, which had pledged never to censor the internet, blocked prominent blogs and news websites for the first time. The sites had reported on a billion-dollar corruption scandal implicating Prime Minister Najib Razak. The content-sharing platform Medium was blocked completely after one of the previously affected sites used it to repost content.
- News and opinion on **conflict**, terrorism, or outbreaks of violence were subject to censorship in 27 out of 65 countries. Sensitivity about ongoing conflict resulted in legitimate content being censored. In May 2016, British journalist Martyn Williams challenged South Korean regulators for blocking his website, North Korea Tech.
- **Social commentary** on issues including history and natural disasters was censored in 21 out of 65 countries. In August 2015, Ecuador prohibited independent reporting on the newly active volcano Cotopaxi. Citizens turned to social media for news, and as a result the government announced legal actions against users for "unscrupulous" comments on social networks. In China, discussion of the 1989 crackdown on prodemocracy protesters in Tiananmen Square is censored so comprehensively that internet users in mid-2015 reported being unable to make online financial transfers in denominations of 6 or 4, numbers which connote the crackdown's June 4 anniversary.
- Twenty out of 65 countries censored **blasphemy**, or content considered insulting to religion, suppressing legitimate commentary about religious and other issues. In 2016, internet service providers in India were ordered to block jihadology.net, an academic repository of primary sources about Islamist militancy. In Brazil, artist Ana Smiles was ordered to remove images of religious figurines dressed as superheroes or famous artists from social media.
- Information by or about particular **ethnic groups** was subject to censorship in 13 out of 65 countries. In Turkey, where fighting between security forces and the Kurdistan Workers' Party (PKK) has escalated, dozens of websites and Twitter accounts belonging to journalists reporting on the conflict have been censored.

Images draw greater scrutiny

Images, a vivid and immediate way of communicating information online, became a new priority for censors around the world in the past year. Several governments blocked platforms that allow users to exchange images easily in a bid to contain social and political protests. In Vietnam, Instagram was blocked along with Facebook during environmental protests in 2016, after both tools were used to organize and share images of fish killed en masse by industrial pollution.

A 22 year-old student in Egypt was sentenced to three years in prison for posting this photo depicting President Abdel Fattah al-Sisi with Mickey Mouse ears on Facebook.

World leaders proved particularly sensitive to altered images of themselves circulating on social media. In Egypt, a photo depicting President Abdel Fattah al-Sisi with Mickey Mouse ears resulted in a three-year prison term for the 22-year-old student who posted it on Facebook. Three people in Zimbabwe were arrested for photos of President Robert Mugabe that they shared in satirical social media posts.

Journalists were often targeted for disseminating images as part of their work. Police in Kenya arrested journalist Yassin Juma for using Facebook to report on and share photos of casualties in an attack on Kenyan forces stationed in Somalia. Egyptian photojournalist Ali Abdeen was arrested in April 2016 for covering protests against the transfer of Egyptian islands to Saudi Arabia. He was convicted in May of inciting illegal protests, publishing false news, and obstructing traffic, though his employers at the news website El-Fagr confirmed that he was working on assignment.

Security measures threaten free speech and privacy

In both democratic and authoritarian countries, counterterrorism measures raised the likelihood of collateral damage to free speech, privacy rights, and business operations. Although in some cases the actions were meant to address legitimate security concerns, 14 of the 65 countries assessed in *Freedom on the Net* approved new national security laws or policies that could have a disproportionately negative effect on free speech or privacy, with especially threatening consequences for government critics and journalists in countries that lack democratic checks and balances. Meanwhile, high-profile terrorist attacks in Europe and the United States led to increased pressure on technology companies to cooperate more closely with law enforcement regarding access to user data.

Broad antiterrorism laws lead to unjust penalties

In numerous authoritarian countries, officials enforced antiterrorism and national security laws in a manner that produced excessive or entirely inappropriate punishments for online activity. In the gravest cases, such laws were used to crack down on nonviolent activists, prominent journalists, and ordinary citizens who simply questioned government policies or religious doctrine.

In December 2015, a court in Russia handed down the first maximum sentence of five years in prison for extremism to blogger Vadim Tyumentsev, who was charged for posting videos that criticized pro-Kremlin separatists in eastern Ukraine and called for the expulsion of refugees coming to Russia from the Ukrainian regions of Donetsk and Luhansk. In July 2016, a new Russian law increased the maximum prison term for justifying or inciting terrorism to seven years. Penalties are even harsher in Pakistan, where antiterrorism courts sentenced two men in separate cases to 13 years in prison for promoting sectarian hatred on Facebook. A lawyer for one of the men said he had only “liked” the post in question, which was described as “against the belief of Sunni Muslims.”

Overly broad definitions of terrorism often resulted in spurious convictions. In Jordan, activist Ali Malkawi was arrested for criticizing the stance of Arab and Muslim leaders regarding the plight of Myanmar’s persecuted Rohingya minority. He was sentenced to three months in jail under the antiterrorism law for “disturbing relations with a friendly state.” Ethiopian blogger Zelalem Workagenehu was found guilty of terrorism and sentenced to over five years in prison in May for facilitating a course on digital security.

In some cases, journalists were branded as terrorists for independently documenting civil strife and armed conflicts. Sayed Ahmed al-Mousawi, an award-winning Bahraini photojournalist, was sentenced to 10 years in prison under an antiterrorism law in November 2015 due to his role in covering antigovernment protests and providing SIM cards to alleged “terrorists.” Hayri Tunç, a Turkish journalist for the news site *Jiyan*, was sentenced to two years in prison for creating “terrorist propaganda” through his tweets, Facebook posts, and YouTube videos related to the conflict between the state and Kurdish militants.

Pressure to enable backdoor access

In democracies, where the definition of terrorism tends to have a narrower scope, debate has focused on the ability of intelligence and law enforcement agencies to prevent and prosecute terrorist attacks. As technology companies develop stronger privacy safeguards for their users, they have clashed with government entities attempting to gather information on suspected terrorists.

Two New York Police Department (NYPD) officers stand guard near the Apple store on Fifth Avenue in New York during an anti-government demonstration on February 23, 2016. (Jewel Samad/Getty Images).

A United States district court ordered Apple to create new software that could bypass its own security measures and access a locked iPhone used by a perpetrator of the December 2015 terrorist attack in San Bernardino, California. Apple chief executive Tim Cook warned in a public letter that doing so would set a dangerous domestic legal precedent, embolden undemocratic governments to make similar requests, and make Apple products more vulnerable to hackers. U.S. authorities eventually dropped the case after experts were able to unlock the iPhone without Apple's help, leaving the broader legal issue unresolved.

Similarly, high-profile terrorist attacks in Europe have increased pressure to bolster the surveillance powers of government agencies tasked with disrupting future plots. France has extended a state of emergency since a major attack struck Paris in November 2015, authorizing security agencies to monitor and detain individuals with little judicial oversight. Germany passed a law mandating the retention of telecommunications data by providers for up to 10 weeks, despite fierce protests from the opposition and a 2014 ruling by the EU's Court of Justice that such blanket requirements contravene fundamental rights. In August 2016, interior ministers from both countries called on the European Commission to draft an EU-level framework for compelling the makers of encrypted chat apps to hand over decrypted data in terrorism cases.

Authoritarian states have also joined the fray, but with far fewer scruples about individual rights. In Russia, for example, a draconian antiterrorism law passed in June 2016 requires all "organizers of information online"—which in theory could include local service providers as well as foreign social media companies—to provide the Federal Security Service (FSB) with tools to decrypt any information they transmit, essentially mandating backdoor access. The law will also require service providers to keep users' metadata for up to three years and the content of users' communications—calls, texts, images, videos, and other data—for up to six months.

Faced with growing pressure to comply with government requests, some tech companies have pushed back. Shortly after the Apple case, Microsoft sued the United States over the right to tell customers when data stored on the company's servers has been handed over to government agencies. (Twitter initiated a similar lawsuit in 2014.) And in March 2016, roughly a billion people received a huge boost in their cybersecurity when Facebook rolled out end-to-end encryption for all WhatsApp users, incorporating technology from the makers of the security app Signal. However, such resistance is nearly impossible in countries that lack free and independent judicial institutions. Companies operating in authoritarian settings have little choice but to leave the market, comply with state demands, or risk blocking, closure, or imprisonment of their local staff.

Exploiting encryption's weakest links

Even when back doors are not installed, state entities and other actors have found ways to overcome cybersecurity and privacy safeguards. This year several governments exploited one of the weakest links in some encrypted apps: SMS authentication. Many platforms currently allow users to confirm their identity through a text message sent to their phone, whether to augment password security, replace forgotten passwords, or activate a new account. German agents reportedly intercepted these messages—which are unencrypted by default—in order to access the Telegram accounts of a neo-Nazi terrorist group suspected of plotting to attack a refugee shelter and assassinate Muslim clerics. The same technique was used in attempts to spy on nonviolent political and social activists in Egypt, Iran, and Russia over the past year. Companies and activists have recommended turning off SMS authentication in favor of code-generator apps.

Another potential weak link can be found in certificates, the small files that allow encrypted web traffic to travel to its destination and be decrypted for access by the intended recipient. Kazakhstan passed a new law requiring users and providers to install a “national security certificate” on all devices. While questions remain about how the requirement will be implemented in practice, observers worry that the measure will undermine cybersecurity for all Kazakh users by allowing security agencies or hackers to intercept and decrypt traffic before it reaches end users. If the law is successful, repressive countries around the world will look to Kazakhstan as a model for circumventing encryption in the name of national security.

New heights in digital activism

As governments around the world impose new restrictions on internet freedom, it is worth remembering what is at stake. The present crackdown comes as digital platforms are being used in new and creative ways to advocate for change and, in many cases, save lives. Internet advocacy had real-world results in both democracies and authoritarian settings over the past year, and its impact was often most pronounced in countries where the information environment was more open online than off. In over two-thirds of the countries examined in this study, there was at least one significant example of individuals producing a tangible outcome by using online tools to fight for internet freedom, demand political accountability, advance women’s rights, support victims of unjust prosecution, or provide relief to those affected by natural disasters.

Fighting for internet freedom and digital rights

Social media were used effectively to fight for internet freedom in a variety of countries over the past year. In Thailand, over 150,000 people signed a Change.org petition against a government plan to centralize the country’s internet gateways, which would strengthen the authorities’ ability to monitor and censor online activity. As a result, the government announced that it had scrapped the plan, though skeptical internet users remain vigilant.

Using the hashtag #NoToSocialMediaBill, Nigerian digital rights organizations launched a multifaceted campaign to defeat a “Frivolous Petitions Prohibition Bill” that threatened to constrain speech on social media. Alongside significant digital media activism, civil society groups organized a march on the National Assembly, gathered signatures for a petition presented during a public hearing on the bill, and filed a lawsuit at the Federal High Court in Lagos, all of which contributed to the bill’s withdrawal in May 2016. India’s telecommunications regulator banned differential pricing schemes in February after more than a million comments were submitted online to protest companies that charge consumers different prices for select content or applications.

Protesting governments and demanding accountability

Social media were also used to combat corruption, wasteful spending, or government abuse. Movements like Lebanon’s #YouStink or #ElectricYerevan in Armenia channeled citizens’ anger over bread-and-butter issues—a garbage crisis and energy price hikes, respectively—into sustained protests that brought thousands of people to the streets and extracted responses from the government. Citizens in Kyrgyzstan criticized the parliament’s plan to spend some US$40,000 on 120 new chairs to replace those purchased only five years earlier. The campaign, called #120Кресел (120Chairs), received extensive coverage on Twitter and through news outlets, and lawmakers subsequently abandoned the plan.

Even in some of the world’s most closed societies, individuals have used smartphones to record and publicize instances of abuse by state officials. After a video showing abuse at a military academy went viral in Myanmar, public outrage forced the military to launch a high-level investigation, an unprecedented gesture toward accountability from the country’s most untouchable institution. In Saudi Arabia, the head of Riyadh’s Committee for the Promotion of Virtue and the Prevention of Vice was dismissed in a bid to quell popular unease over a video in which members of the so-called morality police chased a girl outside a mall in the Saudi capital.

Venezuelans rely on secure messaging tools to exchange information about scarce goods. Online content about currency exchange rates is pervasively censored. Getty Images.

Defending women’s rights around the globe

Several countries featured notable internet-based campaigning for women’s rights. A Jordanian activist launched a popular online petition asking the parliament to amend Article 123 of the civil law, which requires that a male guardian be present for children to be admitted at hospitals. The National Council for Family Affairs, chaired by Queen Rania, later drafted legislation that created an exception in cases of emergency. In Argentina, the alarming rate of femicide and other gender-based violence led to an ongoing campaign, #NiUnaMenos (Not One Less), that has generated almost 300,000 tweets and inspired hundreds of thousands of people to demonstrate on June 3 of 2015 and 2016.

Disaster relief and saving lives during wartime

There were numerous instances during the year of social media and communication apps enabling crucial information-sharing that was credited with saving lives. Citizens and organizations have used digital tools to organize relief efforts, solicit donations, and disseminate information about rescue operations. In Sri Lanka, taxi apps like PickMe introduced an SOS button that allowed customers trapped in flood-affected areas to mark their location for rescue. And some of the most extraordinary uses of social media took place in Syria, where online applications have long been vital for citizen journalists and civic activists. The Syrian American Medical Society has used WhatsApp for telemedicine, in one instance guiding a veterinarian who delivered twin babies by caesarean section in the besieged town of Madaya.

Such examples of activism indicate that the internet is an indispensable tool for promoting social justice and political liberty, used by citizens worldwide to fight for their rights, demand accountability, and amplify marginalized voices. This is precisely why authoritarian governments are intensifying their efforts to impose control, and why democratic societies must simultaneously defend internet freedom abroad and uphold their own standards at home.

Donors

U.S. State Department’s Bureau of Democracy
Human Rights and Labor (DRL)
Google
Schloss Family Foundation
Dutch Ministry of Foreign Affairs
Facebook
Internet Society
Yahoo
Twitter

Research Team

Sanja Kelly, Director, Freedom on the Net

Mai Truong, Program Manager (Africa)

Adrian Shahbaz, Research Manager (MENA)

Madeline Earp, Senior Research Analyst (Asia)

Jessica White, Research Analyst (Latin America and the EU)

Rose Dlougatch, Senior Research Associate (Eurasia)

Report Authors and Advisers

Argentina: Eduardo Ferreyra, Valeria Milanes, Jeannette Torrez, Leandro Ucciferri, Free Expression & Privacy team, Association for Civil Rights (ADC)

Armenia: Artur Papyan, Internet Journalist at RFE/RL, and media development consultant

Australia: Dr. Alana Maurushat, Senior Lecturer, Faculty of Law, and Co-Director, Cyberspace Law and Policy Community, The University of New South Wales

Azerbaijan: Arzu Geybulla, Azerbaijani journalist

Brazil: Fabrício Bertini Pasquot Polido, Professor, Law School of the Federal University of Minas Gerais, and Head of the Center for International Studies on Internet, Innovation, and Intellectual Property (GNET); Carolina Rossini, Vice President of International Policy, Public Knowledge, and Board Member, Open Knowledge Foundation, InternetLab, and CodingRights

Cambodia: Sopheap Chak , Executive Director, Cambodian Center for Human Rights, and human rights blogger

Canada: Allen Mendehlson, Canadian lawyer specializing in internet and technology law

Colombia: Law, Internet, and Society Group, Fundación Karisma

Cuba: Ernesto Hernández Busto , Cuban journalist and writer

Estonia: Linnar Viik, Lecturer, Board Member, Estonian IT College

France: Jean-Loup Richet, Researcher, University of Nantes

Georgia: Teona Turashvili, E-Governance Direction Lead, Institute for Development of Freedom of Information (IDFI)

Germany: Philipp Otto, Founder and Head, iRights.Lab think tank and iRights.Media publishing house, Editor in Chief, iRights.info, political strategist, advisor to the German government and companies; Henning Lahmann, Policy Analyst, iRights.Lab

Hungary:Dalma Dojcsák and Máté Szabó, Hungarian Civil Liberties Union

Iceland: Caroline Nellemann, independent consultant, specialist in digital media and civic engagement

India: Sarvjeet Singh, Programme Manager, Centre for Communication Governance at National Law University, Delhi; Parul Sharma, Analyst, Center for Communication Governance; assistance from Nishtha Sinha and Vaibhav Dutt, Students, B.A., LL.B. (Hons.), National Law University

Indonesia: Indriaswati Dyah Saptaningrum, Senior Researcher, ELSAM (The Institute for Policy Research and Advocacy)

Iran: Kyle Bowen and Mahmood Enayat, Small Media

Italy: Giampiero Giacomello, Associate Professor of International Relations, University of Bologna

Japan: Dr. Leslie M. Tkach-Kawasaki, Associate Professor, University of Tsukuba

Jordan: Lina Ejeilat, Co-founder and Executive Editor, 7iber

Kazakhstan: Adilzhan Nurmakov, Senior Lecturer, KIMEP University

Kenya: Grace Githaiga, Associate, Kenya ICT Action Network (KICTANet)

Kyrgyzstan: Artem Goryainov, IT Programs Director, Public Foundation CIIP

Lebanon: Firas Talhouk, Program Manager, Public Policy Lab at the Issam Fares Institute for Public Policy and International Affairs, American University of Beirut

Libya: Fadil Aliriza, journalist, researcher, political analyst, and Tunisia Project Manager, Carnegie Endowment for International Peace

Malawi: Gregory Gondwe, Bureau Chief, Times Media Group, Malawi

Malaysia: K Kabilan, Managing Editor, BeritaDaily.com, and online media consultant

Mexico: Jorge Luis Sierra, Knight International Journalism Fellow, International Center for Journalists, and award-winning Mexican journalist

Morocco: Bouziane Zaid, Associate Professor of Media and Communication, Al Akhawayn University in Ifrane

Myanmar: Min Zin, Executive Director, Institute for Strategy and Policy: Myanmar

Nigeria: ‘Gbenga Sesan, Executive Director, Paradigm Initiative Nigeria

Pakistan: Nighat Dad, Executive Director, Digital Rights Foundation, Pakistan; Adnan Ahmad Chaudhri, Associate Researcher, Digital Rights Foundation

Russia: Darya Luganskaya, freelance journalist

Singapore: Cherian George, Associate Professor, School of Communication, Hong Kong Baptist University

South Africa: Zororo Mavindidze, Senior Researcher, Freedom of Expression Institute

South Korea: Dr. Yenn Lee, Doctoral Training Advisor, SOAS, University of London (School of Oriental and African Studies)

Sri Lanka: N. V. Nugawela, consultant and researcher

Sudan: Azaz Elshami, independent researcher and development consultant

Syria: Dlshad Othman, information security expert

Uganda: Lillian Nalwoga, Policy Officer, CIPESA, and President, Internet Society Uganda Chapter

Ukraine: Tetyana Lokot, Ukrainian media researcher, Lecturer in Journalism, Dublin City University

United Kingdom: Aaron Ceross, Researcher in Cyber Security, University of Oxford

United States: Laura Reed, independent researcher

Uzbekistan: Dr. Zhanna Hördegen, Research Associate, University Research Priority Program (URPP) Asia and Europe, University of Zurich, and independent consultant

Venezuela: Raisa Urribarri, Director, Communications Lab for Teaching, Research and Community Extension (LIESR) at the University of Los Andes

Zambia: Brenda Bukowa, Lecturer and Researcher, Department of Mass Communication, University of Zambia

The analysts for the reports on Angola, Bahrain, Bangladesh, Belarus, China, Ecuador, Egypt, Ethiopia, The Gambia, Jordan, Rwanda, Philippines, Saudi Arabia, Thailand, Tunisia, Turkey, United Arab Emirates, Vietnam and Zimbabwe are independent internet researchers who have asked to remain anonymous.

Freedom House would also like to thank the Internet Society (ISOC) and ISOC country chapters representatives -- including: Athena Morgan, ISOC Kenya chapter; Amrita Choudhury, Treasurer, ISOC India-Delhi Chapter; and Simbarashe Machiridza, ISOC Zimbabwe chapter; as well as ISOC chapter representatives who have asked to remain anonymous -- for providing valuable feedback on Freedom on the Net 2016 country reports.

Freedom House is solely responsible for the content of this report.

Report Navigation

- Silencing the Messenger: Communication Apps Under Pressure
- 2016 Country Scores
- Key Internet Controls by Country
- Methodology
- About *Freedom on the Net*

Country Reports

- Select a Country Report - Angola Argentina Armenia Australia Azerbaijan Bahrain Bangladesh Belarus Brazil Cambodia Canada China Colombia Cuba Ecuador Egypt Estonia Ethiopia France Gambia, The Georgia Germany Hungary Iceland India Indonesia Iran Italy Japan Jordan Kazakhstan Kenya Kyrgyzstan Lebanon Libya Malawi Malaysia Mexico Morocco Myanmar Nigeria Pakistan Philippines Russia Rwanda Saudi Arabia Singapore South Africa South Korea Sri Lanka Sudan Syria Thailand Tunisia Turkey Uganda Ukraine United Arab Emirates United Kingdom United States Uzbekistan Venezuela Vietnam Zambia Zimbabwe

Downloads

- Report PDF
- Report + 65 Country Reports
- Report Graphics