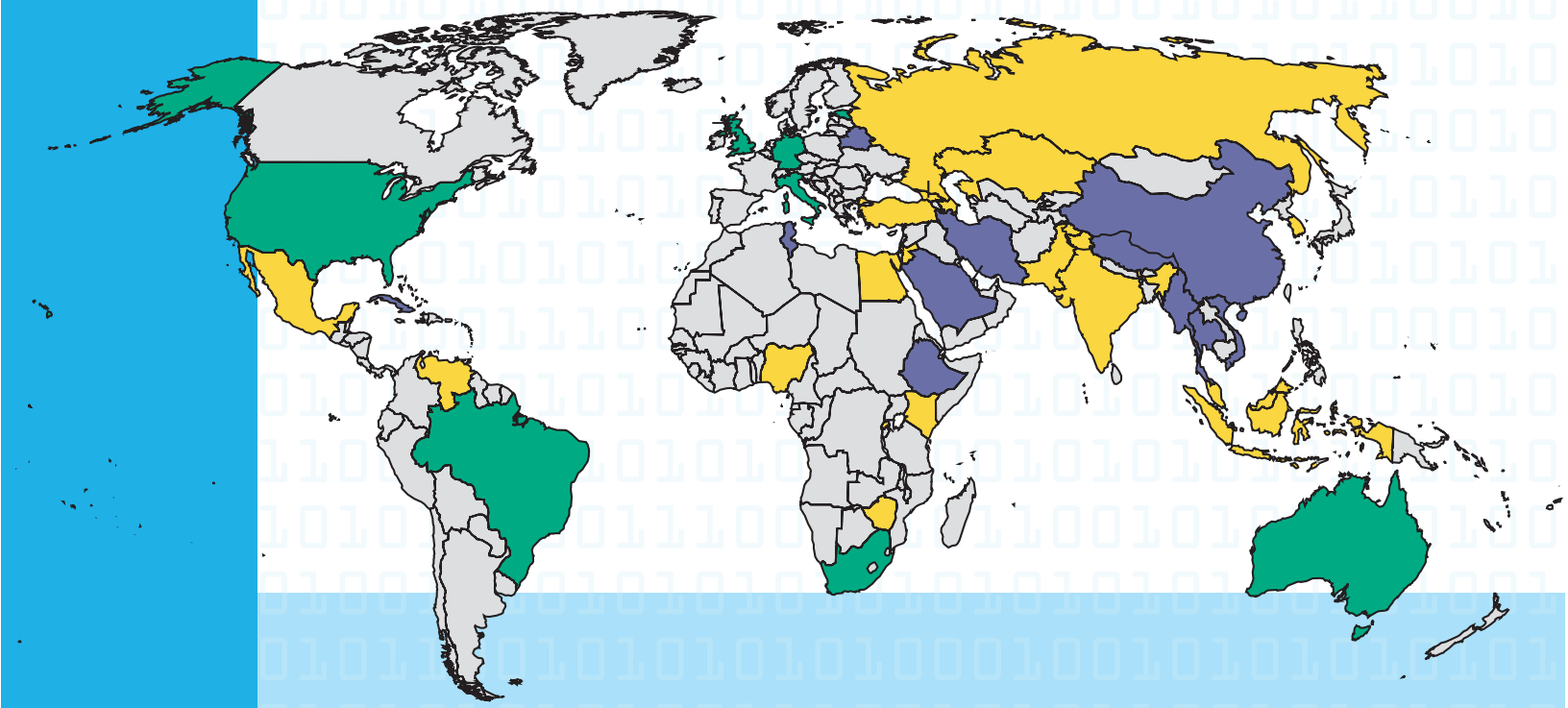
FREEDOM HOUSE

FREEDOM ON THE NET 2011

A GLOBAL ASSESSMENT OF INTERNET AND DIGITAL MEDIA



UNDEF The United Nations Democracy Fund

FREEDOM ON THE NET 2011

A Global Assessment of Internet and Digital Media

Sanja Kelly

Sarah Cook

EDITORS

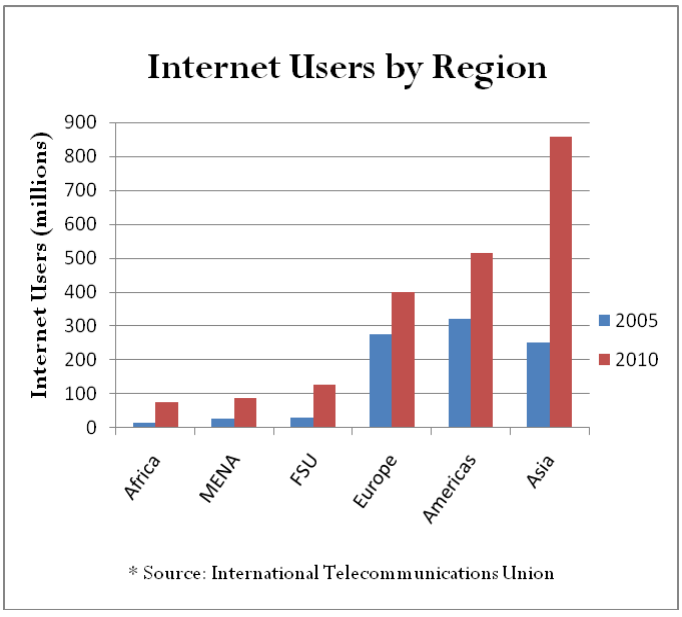
April 18, 2011

NEW TECHNOLOGIES, INNOVATIVE REPRESSION: Growing Threats to Internet Freedom

By Sanja Kelly and Sarah Cook

Over the past decade, and particularly in the last few years, the influence of the internet as a means to spread information and challenge government-imposed media controls has steadily expanded. This mounting influence directly corresponds to the growth in the number of users around the world: over two billion people now have access to the internet, and the figure has more than doubled in the past five years. However, as more people use the internet to communicate, obtain information, socialize, and conduct commerce, governments have stepped up efforts to regulate, and in some instances tightly control, the new medium. Reports of website blocking and filtering, content manipulation, attacks on and imprisonment of bloggers, and cyberattacks have all increased sharply in recent years.

To illuminate the nature of the emerging threats and identify areas of growing opportunity, Freedom House has conducted a comprehensive study of internet freedom in 37 countries around the globe. An earlier, pilot version was published in 2009, covering a sample of 15 countries. The new edition, *Freedom on the Net 2011*, assesses a wider range of political systems, while tracking improvements and declines in the countries examined two years ago. Over 40 researchers, most of whom are based in the countries they examined, contributed to the project by researching laws and practices relevant to the internet, testing accessibility of select websites, and interviewing a wide range of sources. Although the study's findings indicate that the threats to internet freedom are growing and have become more diverse, they also highlight a pushback by citizens and activists who have found ways to sidestep some of the restrictions and use the power of new internet-based platforms to promote democracy and human rights.



When the internet first became commercially available in the 1990s, very few restrictions on online communications and content were in place. Recognizing the economic potential of the new medium, many governments started investing heavily in telecommunications infrastructure, and internet-service providers (ISPs) sought to attract subscribers by creating online chat rooms and building communities of users around various topics of interest. Even the authorities in China, which today has the most sophisticated regime of internet controls, exerted very little oversight in the early days. However, as various dissident groups in the late 1990s began using the

internet to share information with audiences inside and outside the country, the government devoted tremendous human and material resources to the construction of a multilayered surveillance and censorship apparatus. Although China represents one of the most severe cases, similar dynamics are now becoming evident in many other countries.

Indeed, the country reports and numerical scores in this study reveal that a growing number of governments are moving to regulate or restrict the free flow of information on the internet. In authoritarian states, such efforts are partly rooted in the existing legal frameworks, which already limit the freedom of the traditional media. These states are increasingly blocking and filtering websites associated with the political opposition, coercing website owners into taking down politically and socially controversial content, and arresting bloggers and ordinary users for posting information that is contrary to the government's views. Even in more democratic countries—such as Brazil, India, Indonesia, South Korea, Turkey, and the United Kingdom—internet freedom is increasingly undermined by legal harassment, opaque censorship procedures, or expanding surveillance. The spread and intensification of internet controls in each country that showed decline generally conformed to one of the following three patterns:

Initial signs of politically motivated internet controls: In several countries that were previously free from most internet controls, the first signs of politicized censorship and user rights violations emerged, often in the period before or during elections. Many of these incidents represented the first time that a website in the country had been blocked, a user detained, or a restrictive law passed. This dynamic was particularly evident in Venezuela, Azerbaijan, Jordan, and Rwanda. In Venezuela, for example, users subscribing to internet services through the state-owned telecommunications firm CANTV reported that they were unable to access opposition-oriented blogs and a popular news site in the days surrounding parliamentary elections in September 2010. In Azerbaijan in 2009, the authorities temporarily blocked several websites that lampooned the president, and jailed two youth activists who posted a video that mocked the government.

Acceleration and institutionalization of internet controls: In countries where the authorities had already shown some tendency toward politically motivated controls over the internet, the negative trend accelerated dramatically, and new institutions were created specifically to carry out censorship. In Pakistan, for example, where temporary blocks have been common in recent years, a new Inter-Ministerial Committee for the Evaluation of Websites was established in mid-2010 to flag sites for blocking based on vaguely defined offenses against the state or religion. In Thailand, the government has long blocked internet content and taken legal action against users, particularly those posting information that is critical of the monarchy. However, the number of detained offenders and blocked sites sharply increased over the last two years, particularly while top officials had the authority to extrajudicially order blockings under a state of emergency that lasted from April to December 2010.

Strengthening of existing internet-control apparatus: Even in countries with some of the most robust censorship and internet surveillance systems in the world, measures were taken to eliminate loopholes and further strengthen the apparatus. In China, blogs on political and social issues were shut down, the space for anonymous communication has dwindled, and the

government has stepped up efforts to counter circumvention tools. In Bahrain, Iran, Ethiopia, and Tunisia, intensified censorship or user arrests came in the context of popular protests or contentious elections. Following the June 2009 elections in Iran, the country's centralized filtering system evolved to the point of being able to block a website nationwide within a few hours, and over 50 bloggers have been detained. In Vietnam, in addition to blocking websites, restricting some social-networking tools, and instigating cyberattacks, the authorities displayed their muscle by sentencing four activists to a total of 33 years in prison for using the internet to report human rights violations and express prodemocracy views.

The new internet restrictions around the globe are partly a response to the explosion in the popularity of advanced applications like Facebook, YouTube, and Twitter, through which ordinary users can easily post their own content, share information, and connect with large audiences. While mostly serving as a form of entertainment, over the last two years these tools have also played a significant role in political and social activism. In Egypt and Tunisia, for example, democracy advocates have relied heavily on Facebook to mobilize supporters and organize mass rallies. Similarly, Bahraini activists have used Twitter and YouTube to inform the outside world about the government's violent response to their protests. Even in Cuba, one of the most closed societies in the world, several bloggers have been able to report on daily life and human rights violations.

Many governments have started specifically targeting these new applications in their censorship campaigns. In 12 of the 37 countries examined, the authorities consistently or temporarily imposed total bans on YouTube, Facebook, Twitter, or equivalent services. Moreover, the increased user participation facilitated by the new platforms has exposed ordinary people to some of the same punishments faced by well-known bloggers, online journalists, and human rights activists. Among other recent cases, a Chinese woman was sent to a labor camp over a satirical Twitter message, and an Indonesian housewife faced high fines for an e-mail she sent to friends complaining about a local hospital. Because new technologies typically attract the young, some of those arrested have been teenagers, including an 18-year old Iranian blogger writing about women's rights and a 19-year old Tibetan detained after looking at online photographs of the Dalai Lama.

In 23 of the 37 countries assessed, a blogger or other internet user was arrested for content posted online.

KEY FINDINGS

The 2011 edition of *Freedom on the Net* identifies a growing set of obstacles that pose a common threat to internet freedom in many of the countries examined. Of the 15 countries covered in the pilot, a total of 9 registered score declines over the past two years. The newly added countries lack earlier scores for comparison, but conditions in at least half of them suggest a negative trajectory, with increased government blocking, filtering, legal action, and intimidation to prevent users from accessing unfavorable content. In cases where these tactics are deemed ineffective or inappropriate, authorities have turned to cyberattacks, misinformation, and other indirect methods to alter the information landscape.

Political Content Increasingly Blocked, Transparency Lacking

Governments around the world have responded to soaring internet penetration rates and the rise of user-generated content by establishing mechanisms to block what they deem to be undesirable information. In many cases, the censorship targets content involving illegal gambling, child pornography, copyright infringement, or the incitement of hatred or violence. However, a large number of governments are also engaging in deliberate efforts to block access to information related to politics, social issues, and human rights.

Of the 37 countries examined, the governments of 15 were found to engage in substantial blocking of politically relevant content. In these countries, instances of websites being blocked are not sporadic or limited in scope. Rather, they are the result of an apparent national policy to restrict users' access to dozens, hundreds, or most often thousands of websites, including those of independent and opposition news outlets, international and local human rights groups, and individual blogs, online videos, or social-networking groups.

Countries with substantial censorship of political or social issues in 2009–10:

Bahrain, Belarus, Burma, China, Cuba, Ethiopia, Iran, Kazakhstan, Pakistan, Saudi Arabia, South Korea, Thailand, Tunisia, Turkey, Vietnam

Website blocking is typically implemented by ISPs acting on instructions from a government agent, judge, or other appointed entity, whose orders may apply to a particular domain name, an internet-protocol (IP) address, or a specific URL. ISPs keep track of and periodically receive updates on the resulting blacklists of banned sites. In a small number of countries, the filtering technology employed is more sophisticated, and can scan users' browsing requests for certain banned keywords. Keyword filtering is much more nuanced, enabling access to a given website but not to a particular article containing a sensitive keyword in its URL path. Among the countries studied, China, Iran, and Tunisia are known to have such systems in place. In China, which boasts the world's most comprehensive censorship apparatus, keyword filtering is evident in instant-messaging services as well, having been built into the software of popular messaging programs like TOM Skype and QQ.

Two of the countries categorized by Freedom House as electoral democracies—Turkey and South Korea—were also found to engage in substantial political censorship. In Turkey, a range of advanced web applications were blocked, including the video-sharing website YouTube, which was not accessible in Turkey from May 2008 to October 2010. South Korean authorities blocked access to an estimated 65 North Korea–related sites, including the official North Korean Twitter account, launched in August 2010. Meanwhile, the governments of Australia, Indonesia, and Italy introduced proposals that would enable automated filtering by ISPs, create a state-led multimedia content screening entity, and extend prescreening requirements from television broadcasting to video-hosting websites, respectively. By the end of 2010, these proposals had been set aside or amended to remove the most egregious requirements.

One aspect of censorship was evident across the full spectrum of countries studied: the arbitrariness and opacity surrounding decisions to restrict particular content. In most nondemocratic settings, there is little government effort to inform the public about which content is censored and why. In many cases, authorities avoid confirming that a website has been

deliberately blocked and instead remain silent or cite "technical problems." Saudi Arabia does inform users when they try to access a blocked site, and the rules governing internet usage are clearly articulated on government portals, but as in many countries, the Saudi authorities often disregard their own guidelines and block sites at will. Even in more transparent, democratic environments, censorship decisions are often made by private entities and without public discussion, and appeals processes may be onerous, little known, or nonexistent.

The widespread use of circumvention tools has eased the impact of content censorship and at times undermined it significantly. Such tools are particularly effective in countries with a high degree of computer literacy or relatively unsophisticated blocking techniques. For example, YouTube remained the eighth most popular website among Turkish users despite being officially blocked in that country for over two years, and the number of Vietnamese Facebook users doubled from one to two million within a year after November 2009, when the site became inaccessible by ordinary means. Users need special skills and knowledge to overcome blockages in countries such as China and Iran, where filtering methods are more sophisticated and the authorities devote considerable resources to limiting the effectiveness of circumvention tools. Still, activists with the requisite abilities managed to communicate with one another, discuss national events in an uncensored space, and transmit news and reports of human rights abuses abroad.

Cyberattacks Against Regime Critics Intensify

Some governments and their sympathizers are increasingly using technical attacks to disrupt activists' online networks, eavesdrop on their communications, and cripple their websites. Such attacks were reported in at least 12 of the countries covered in this study. However, attacks perpetrated by nonstate actors for ordinary criminal purposes are also a growing problem, particularly as internet penetration deepens and more users turn to the medium for shopping, banking, and other activities.

China has emerged as a major global source of cyberattacks. Although not all attacks originating in the country have been explicitly traced back to the government, their scale, organization, and chosen targets have led many experts to conclude that they are either sponsored or condoned by Chinese military and intelligence agencies. The assaults have included denial-of-service (DoS) attacks on domestic and overseas human rights groups, e-mail messages to foreign journalists that carry malicious software capable of spying on the recipient's computer, and large-scale hacking raids on the information systems of over 30 financial, defense, and technology companies, most of them based in the United States. In addition, independent analysts have detected cyberespionage networks that extend to 103 countries as part of an effort to spy on the Tibetan government-in-exile and its foreign government contacts.

As with offline forms of violence and intimidation, governments seem most likely to resort to cyberattacks when their power is threatened by disputed elections or some other political crisis. In Iran, for example, during the mass protests that followed the June 2009 presidential election, many opposition news sites were disabled by intense DoS attacks, and there is technical evidence confirming that government-owned IP addresses were used to launch the assaults. A group calling itself the Iranian Cyber Army, which operates under the command of the Islamic Revolutionary

Guard Corps, managed to hack a number of other sites with a mix of technical methods and forgery.

Similarly, in the wake of fraudulent elections in Belarus in December 2010, the government initiated DoS attacks against opposition websites, dramatically slowing down their connections and in some instances rendering them completely inaccessible. Belarusian authorities also engaged in a type of web forgery designed to confuse users and provide false information. For example, the country's largest ISP, the state-owned Belpak, redirected users from independent media sites to nearly identical clones that provided misleading information, such as the incorrect location of a planned opposition rally.

Countries where websites or blogs of government opponents faced cyber attacks in 2009-2010:

Bahrain, Belarus, Burma, China, Iran, Kazakhstan, Malaysia, Russia, Saudi Arabia, Thailand, Tunisia, Vietnam

The Tunisian regime of President Zine al-Abidine Ben Ali accelerated its hacking activity in the run-up to the January 2011 uprising that drove it from power. Security officials regularly broke into the e-mail, Facebook, and blogging accounts of opposition and human rights activists, either deleting specific material or simply collecting intelligence about their plans and contacts.

Governments Increasingly Exploit Centralized Infrastructure and Built-In Internet Chokepoints

Although it often goes largely unnoticed, centralized government control over a country's connection to international internet traffic poses a significant threat to online free expression and privacy, particularly at times of political turmoil. In about a third of the states examined, the authorities have exploited their control over infrastructure to limit widespread access to politically and socially controversial content, or in extreme cases, to cut off access to the internet entirely.

This centralization can take several forms. In Ethiopia and Cuba, for example, state-run telecommunications companies hold a monopoly on internet service, giving them unchecked control over users' ability to communicate with one another and the outside world. Elsewhere, the state-run company's control of the market is not complete, but its dominance is sufficient to significantly influence people's access to information. Thus when CANTV in Venezuela or Kazakhtelecom in Kazakhstan block a website, it becomes inaccessible to the vast majority of internet users.

As a growing number of governments liberalize the ISP market, such centralization may become less obvious. In countries including Egypt and Belarus, a state-controlled company owns the country's network of copper wires or fiber-optic cables and sells bandwidth downstream to a variety of retail-level ISPs. In China, Vietnam, and Saudi Arabia, an array of three to eight international gateways are available to multiple, economically competitive ISPs, yet ultimate control over the country's connectivity rests with the government.

Of the 37 countries assessed, 19 had at least a partially centralized and government-controlled international connection. Authorities in at least 12 of these were known to have used their leverage to restrict users' access to politically relevant information or engage in widespread

surveillance. Egypt joined the list in January 2011, when officials shut down the internet nationwide for five days in an unsuccessful attempt to curb antigovernment protests. Technicians reportedly cut off almost all international traffic flowing through a tiny number of portals, while ISPs, particularly state-owned Telecom Egypt, removed the routes to Egypt's networks from global routing tables—the mechanism that provides pathways for users' computers to connect to requested websites. The operation was accomplished within the span of one hour.

The Egyptian case demonstrates that at times of political unrest, authoritarian leaders do not hesitate to exploit infrastructural controls to protect their rule, even if it causes massive disruptions to economic activity and personal communications. Several other instances of this "kill switch" phenomenon have occurred in recent years. In 2007, at the height of a wave of popular protests led by Buddhist monks in Burma, state-run ISPs cut off the country's internet connection from September 27 to October 4. More recently, from July 2009 to May 2010, the Chinese authorities severed all connections to the northwestern region of Xinjiang while security forces carried out mass arrests in the wake of ethnic violence. Local government websites and other content hosted within Xinjiang remained accessible, but the region's 20 million residents were cut off from outside information and a range of services used daily by individuals and businesses—including e-mail, instant messaging, and blog-hosting.

Countries with at least partially centralized and government-controlled internet connections:

Azerbaijan, Bahrain, Belarus, Burma, China, Cuba, Egypt, Ethiopia, Iran, Jordan, Kazakhstan, Malaysia, Saudi Arabia, Thailand, Tunisia, Turkey, Venezuela, Vietnam, Zimbabwe

In addition to outright shutdowns, a centralized, state-controlled internet infrastructure facilitates two other types of restrictions: the deliberate slowing of connection speeds and the imposition of a nationwide system of filtering and surveillance. During opposition protests in Iran in the summer of 2009, authorities sharply reduced the speed of network traffic, making it difficult to conduct basic online activities like opening e-mail messages. Uploading a single image could take up to an hour. In early 2011, as protests began flaring up across the Middle East, the Bahraini government selectively slowed down internet connections at newspaper offices, hotels, and homes. The prime example of a centralized filtering system is China's so-called Great Firewall, but other countries, including Iran and Saudi Arabia, also use such systems to enforce nationwide censorship and monitor dissident activity.

Offline Coercion, Online Manipulation Alter Available Information

Rather than relying exclusively on technological sophistication to control internet content, many governments employ cruder but nevertheless effective tactics to delete and manipulate politically or socially relevant information. These methods are often ingenious in their simplicity, in that their effects are more difficult to track and counteract than ordinary blocking.

One common method is for a government official to contact a content producer or host, for example by telephone, and request that particular information be deleted from the internet. In some cases, individual bloggers or webmasters are threatened with various reprisals should they refuse the request. Increasingly, governments and their supporters are also taking advantage of

international hosting platforms' complaint mechanisms to have user-generated content removed. Over the past two years, activists from China, Egypt, Ethiopia, Mexico, and Tunisia found that their YouTube videos or Facebook accounts had been removed or disabled after complaints were filed, apparently by regime supporters. In several of these instances, the content was restored once the problem was brought to the hosting company's attention, but the threat of a blanket ban is sometimes enough to induce large websites to meet governments' specific deletion demands.

A certain set of countries have laws in place to hold content providers and hosts legally responsible for what others post on their sites. Such provisions effectively force the site owner to screen all user-generated content and delete what might be deemed offensive by the authorities. Long-standing laws in China have led internet companies there to employ hundreds of thousands of people responsible for monitoring and censoring online videos, bulletin-board discussions, blog posts, and microblog messages. Nevertheless, in 2009 and 2010, the Chinese authorities adopted various measures to increase pressure on private websites, obliging them to be more vigilant and prevent content from slipping through the cracks. In Thailand, Kazakhstan, Vietnam, and Venezuela, new laws or directives promulgated since 2007 have led to an increase in this type of censorship. In Thailand, for instance, online news outlets are legally responsible for comments posted by readers, and at least one editor is facing criminal charges over reader comments that were critical of the monarchy. In Vietnam and Venezuela, some webmasters and bloggers have disabled the comment feature on their sites to avoid potential liability.

In addition, a range of governments have deployed manpower and resources to proactively manipulate online discussion and bolster progovernment views. Thailand has military units assigned to countering online criticism of the monarchy, and Burma has established a blogging committee in each ministry. Elsewhere, those recruited and paid for such tasks may be ordinary citizens, often youth. Thus China has cadres, known as the "50 Cent Party" for their supposed per-comment fees, who are employed to post progovernment remarks on various online forums, and recruiting advertisements for similar commentators have reportedly begun to appear on Russian job sites. Government-sponsored posts aim not only to defend the leadership and its policies, but also to discredit opposition voices or human rights activists, and to deceive everyday users. During postelection protests in Iran, for example, government supporters posted fake user-generated content to Twitter and YouTube to mislead protesters and journalists.

In a somewhat different manipulation technique, search-engine providers in some countries, most notably China, are required to adjust search results to match government-imposed criteria, for instance by only offering government-affiliated sources on particular topics. In addition to displeasure over a series of cyberattacks, this obligation was at the center of Google's decision to withdraw from China in early 2010.

COUNTRIES AT RISK

After reviewing the findings for the 37 countries covered in this edition of *Freedom on the Net*, Freedom House has identified five that are at particular risk of suffering setbacks related to internet freedom in 2011 and 2012. A number of other countries showed deterioration over the past two years and may continue to decline, but the internet controls in these states—which include Bahrain, China, and Iran—are already well developed. By contrast, in most of the five countries listed below, the internet remains a relatively unconstrained space for free expression, even if there has been some obstruction of internet freedom to date. These countries also typically feature a repressive environment for traditional media, as well as an internet penetration rate of at least 25 percent, meaning the internet is both vitally important and in significant danger of repression.

Thailand

Internet users in Thailand have played a significant role in challenging the political establishment and the role of the monarchy in Thai politics since the military coup of 2006. This has provoked efforts by the government and military to control the free flow of information and commentary online. Although the government has been blocking some internet content since 2003, over the past two years online censorship has increased in both scale and scope, affecting tens of thousands of websites by the end of 2010, including independent news outlets and human rights groups. Restrictions intensified between April and December 2010, when a state of emergency allowed the authorities to extrajudicially block any website. Dozens of people have been charged under various laws for expressing their views online, particularly those that are critical of the monarchy. As of the end of 2010, many of these cases had yet to be decided. The country's political turmoil has continued, and parliamentary elections are tentatively scheduled for December 2011, raising the likelihood of additional backsliding on freedom of expression issues. In a worrying sign, a Thai judge in March 2011 sentenced a web developer to 13 years in prison for comments he posted and for refusing to remove the remarks of others.

Russia

Given the elimination of independent television channels and the tightening of press restrictions since 2000, the internet has become Russia's last relatively uncensored platform for public debate and the expression of political opinions. However, even as access conditions have improved, internet freedom has eroded. In the last two years, the country's first high-profile cases of technical blocking were reported, while tactics for proactively manipulating discussion in the online sphere were refined. Russian bloggers faced increasing intimidation: at least 25 cases of harassment of bloggers by the authorities occurred in 2009 and 2010, including 11 arrests. Greater efforts to increase government influence over the internet are anticipated as the country prepares for parliamentary elections in December 2011 and a presidential election in early 2012. In March 2011, bloggers reportedly uncovered evidence that Russian officials were hiring users to post

comments that would shape a "positive image" of the ruling United Russia party and "form a negative attitude" toward the author of a targeted blog.

Venezuela

While restrictions on broadcast media outlets have grown in recent years, the internet has remained relatively free, with blogs, Facebook, and Twitter becoming important spaces for the free diffusion of information. Opposition groups have used these platforms to mobilize support, and the authorities have responded with some attempts to restrict online content, though to date they have not engaged in large-scale filtering or blogger arrests. There have been periodic interruptions of access to opposition or independent websites, efforts to intimidate websites into censoring the comments of their users, and several prosecutions for information posted on Twitter. Perhaps the most worrying recent development is the passage in December 2010 of laws that increased state control over telecommunications networks and laid the foundation for website managers and service providers to be required to censor the comments of users. President Hugo Chávez had declared in March 2010 that the internet could not be "a free thing where you do and say whatever you want," and progovernment lawmakers were spurred to act in December following opposition gains in September parliamentary elections. The country is now preparing for a presidential election in 2012, and the state-run telecommunications firm CANTV has a record of apparently restricting access to websites and blogs at sensitive times, suggesting that there is a strong possibility of increased censorship and harassment of internet users in the coming months.

Zimbabwe

Internet access remains limited in Zimbabwe, but the number of mobile-phone users has increased rapidly since early 2009, from less than 10 percent of the population to nearly 50 percent by the end of 2010. While the regime of President Robert Mugabe has committed rampant human rights abuses and exercised strict control over the traditional media, the internet is nominally free from government interference. Nevertheless, there are indications that the government has a strong desire to control new information and communication technologies (ICTs), particularly mobile phones. The 2007 Interception of Communications Act allows the authorities to monitor telephone and internet traffic, and requires service providers to intercept communications on the state's behalf. In addition, some content restrictions and registration requirements related to mobile phones have been imposed in recent years. Parliamentary elections are likely to take place in late 2011, internet access via mobile phones is increasing, and there are a number of influential Zimbabwean news sites based in foreign countries, all of which may tempt Mugabe and his ZANU-PF party to increase ICT controls. Given the prevalence of mobile-phone use, this could take the form of censorship of text-messaging or even a "kill switch" action to disable the entire network.

Jordan

Jordan prides itself on offering broader freedom to use the internet than many other Middle Eastern countries. Nonetheless, internet users are aware that their browsing history, comments, and posted materials may be monitored by the authorities. Until recently, the government's interest in maintaining this direct access to public opinion seemed to have outweighed its impulses to control content. In August 2010, despite objections from civil society, the government adopted a new law on cybercrimes that could be used to limit free expression on the internet. For example, it prohibits the posting of any previously nonpublic information relevant to foreign affairs, national security, the national economy, or public safety. Many bloggers and web users have expressed concern that the government could exploit the ambiguous definitions for each of these categories and use the law selectively to silence its critics. Currently, outright blocking of websites by the authorities remains rare, but website owners often remove material after receiving informal complaints via telephone from government officials, and several popular news websites have been subjected to hacking attacks after posting sensitive material. In February 2011, Ammonnews.net was hacked and temporarily disabled after its editors refused to comply with security agents' demands to remove a statement in which Jordanian tribesmen called for democratic and economic reforms.

FREEDOM ON THE NET 2011: GLOBAL SCORES

Freedom on the Net aims to measure each country's level of internet and new media freedom. Each country receives a numerical score from 0 (the most free) to 100 (the least free), which serves as the basis for an internet freedom status designation of Free (0-30 points), Partly Free (31-60 points), or Not Free (61-100).

Ratings are determined through an examination of three broad categories: obstacles to access, limits on content, and violation of user rights.

- **Obstacles to Access:** assesses infrastructural and economic barriers to access; governmental efforts to block specific applications or technologies; and legal, regulatory and ownership control over internet and mobile phone access providers.
- **Limits on Content:** examines filtering and blocking of websites; other forms of censorship and self-censorship; manipulation of content; the diversity of online news media; and usage of digital media for social and political activism.
- **Violations of User Rights:** measures legal protections and restrictions on online activity; surveillance; privacy; and repercussions for online activity, such as legal prosecution, imprisonment, physical attacks, or other forms of harassment.

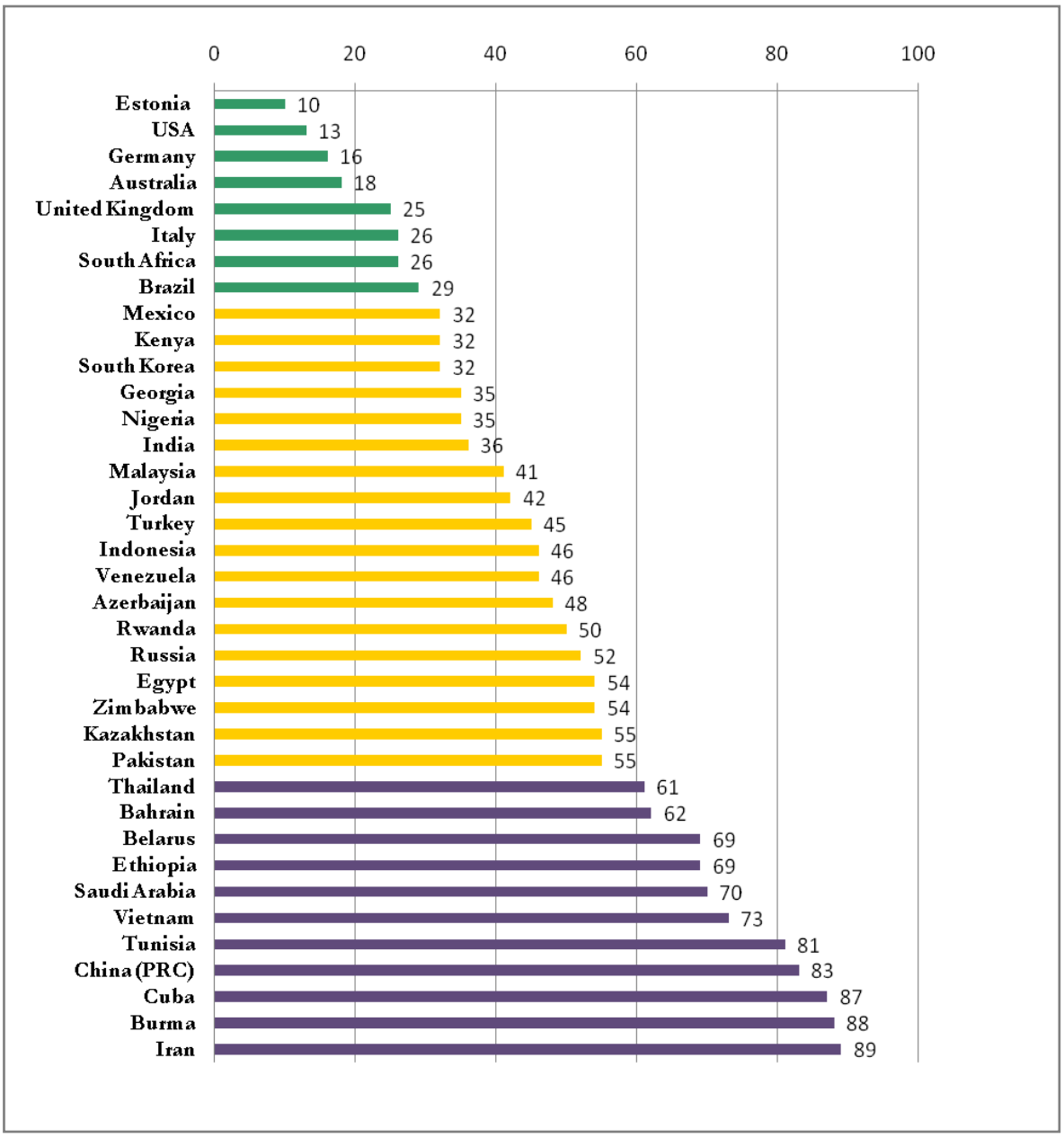
COUNTRY	*FREEDOM ON THE NET* STATUS	*FREEDOM ON THE NET* TOTAL *0-100 Points*	A SUBTOTAL: OBSTACLES TO ACCESS *0-25 Points*	B SUBTOTAL: LIMITS ON CONTENT *0-35 Points*	C SUBTOTAL: VIOLATIONS OF USER RIGHTS *0-40 Points*
Estonia	**Free**	**10**	2	2	6
USA	**Free**	**13**	4	2	7
Germany	**Free**	**16**	4	5	7
Australia	**Free**	**18**	3	6	9
UK	**Free**	**25**	1	8	16
Italy	**Free**	**26**	6	8	12
South Africa	**Free**	**26**	7	9	10

COUNTRY	*FREEDOM ON THE NET* STATUS	*FREEDOM ON THE NET* TOTAL *0-100 Points*	A SUBTOTAL: OBSTACLES TO ACCESS *0-25 Points*	B SUBTOTAL: LIMITS ON CONTENT *0-35 Points*	C SUBTOTAL: VIOLATIONS OF USER RIGHTS *0-40 Points*
Brazil	**Free**	**29**	7	7	15
Kenya	**Partly Free**	**32**	12	9	11
Mexico	**Partly Free**	**32**	12	10	10
South Korea	**Partly Free**	**32**	3	12	17
Georgia	**Partly Free**	**35**	12	10	13
Nigeria	**Partly Free**	**35**	13	10	12
India	**Partly Free**	**36**	12	8	16
Malaysia	**Partly Free**	**41**	9	11	21
Jordan	**Partly Free**	**42**	12	11	19
Turkey	**Partly Free**	**45**	12	16	17
Indonesia	**Partly Free**	**46**	14	13	19
Venezuela	**Partly Free**	**46**	15	13	18
Azerbaijan	**Partly Free**	**48**	15	15	18
Rwanda	**Partly Free**	**50**	14	19	17
Russia	**Partly Free**	**52**	12	17	23
Egypt	**Partly Free**	**54**	12	14	28
Zimbabwe	**Partly Free**	**54**	16	15	23
Kazakhstan	**Partly Free**	**55**	16	22	17
Pakistan	**Partly Free**	**55**	16	17	22

COUNTRY	*FREEDOM ON THE NET* STATUS	*FREEDOM ON THE NET* TOTAL *0-100 Points*	A SUBTOTAL: OBSTACLES TO ACCESS *0-25 Points*	B SUBTOTAL: LIMITS ON CONTENT *0-35 Points*	C SUBTOTAL: VIOLATIONS OF USER RIGHTS *0-40 Points*
Thailand	**Not Free**	**61**	12	23	26
Bahrain	**Not Free**	**62**	11	22	29
Belarus	**Not Free**	**69**	19	23	27
Ethiopia	**Not Free**	**69**	21	26	22
Saudi Arabia	**Not Free**	**70**	14	27	29
Vietnam	**Not Free**	**73**	16	25	32
Tunisia	**Not Free**	**81**	21	28	32
China	**Not Free**	**83**	19	28	36
Cuba	**Not Free**	**87**	24	30	33
Burma	**Not Free**	**88**	23	29	36
Iran	**Not Free**	**89**	21	29	39

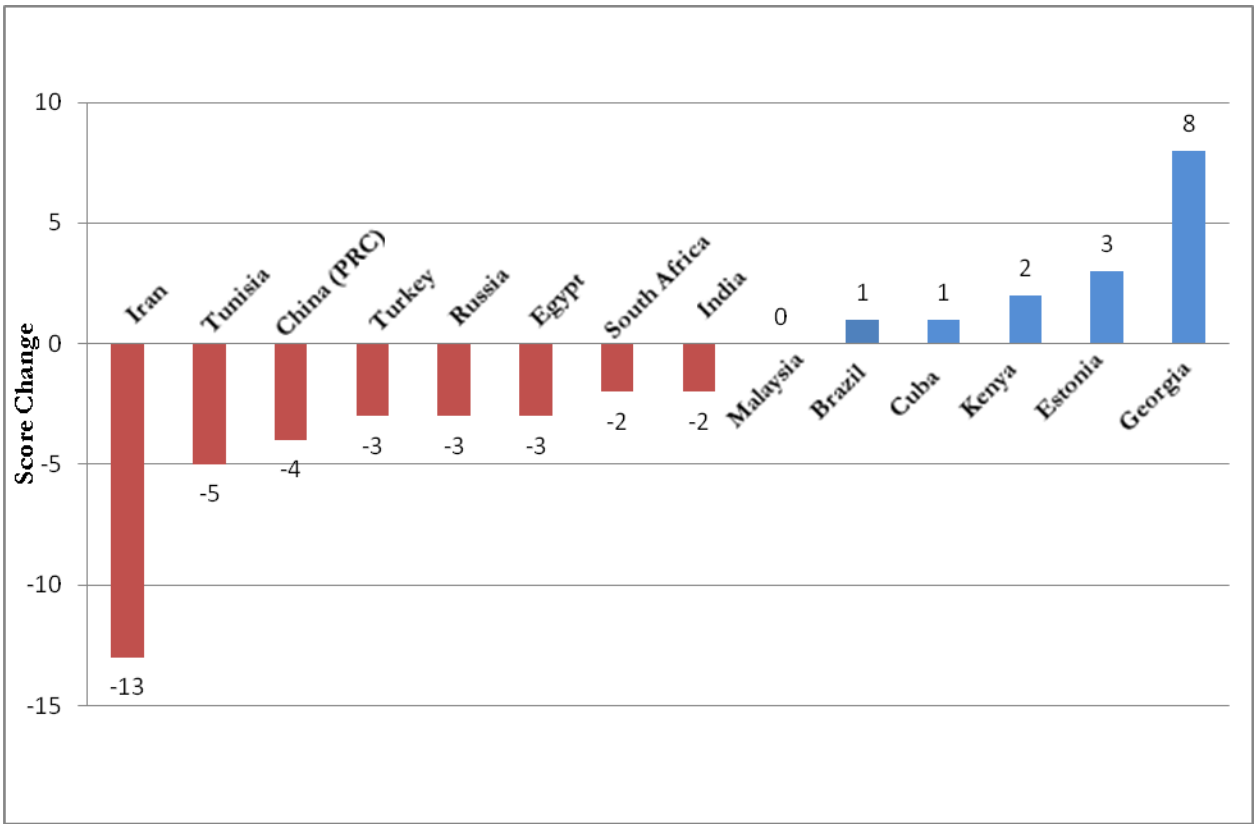
FREEDOM ON THE NET 2011: GLOBAL GRAPHS

37-COUNTRY SCORE COMPARISON (0 Best, 100 Worst)



* A green-colored bar represents a status of **"Free,"** a yellow-colored one, the status of **"Partly Free,"** and a purple-colored one, the status of **"Not Free"** on the *Freedom of the Net* Index.

SCORE CHANGES *FREEDOM ON THE NET 2009 VS. 2011*



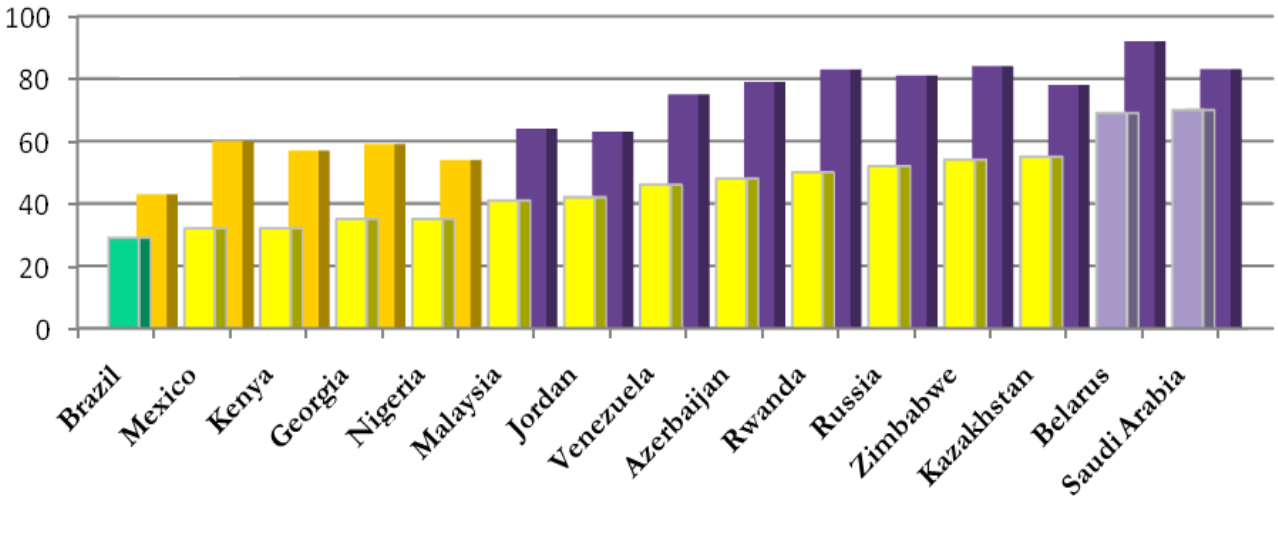
COUNTRY	FOTN 2009	FOTN 2011	TRAJECTORY
Brazil	30	29	↑
China	79	83	↓
Cuba	88	87	↑
Egypt	51	54	↓
Estonia	13	10	↑
Georgia	43	35	↑
India	34	36	↓
Iran	76	89	↓

COUNTRY	FOTN 2009	FOTN 2011	TRAJECTORY
Kenya	34	32	↑
Malaysia	41	41	**No change**
Russia	49	52	↓
South Africa	22	26	↓
Tunisia	76	81	↓
Turkey	42	45	↓
United Kingdom	23	25	↓

COUNTRIES AT RISK: INTERNET FREEDOM VS. PRESS FREEDOM

Among the 37 countries covered in this study, one notable contingent of states were those where the internet remains a relatively unobstructed domain of free expression when compared to a more repressive or dangerous environment for traditional media. This difference is evident from the comparison between a country's score on Freedom House's *Freedom on the Net 2011* assessment and its score on the *Freedom of the Press 2010* study.

The figure below is a graphical representation of this phenomenon, focusing on the 15 countries in this edition where the gap between their performance on the two surveys is 10 points or greater. This difference reflects the potential pressures in both the short and long term on the space for online expression. Among the 15 are several of the states identified as "countries at risk:" Jordan, Russia, Venezuela, and Zimbabwe.

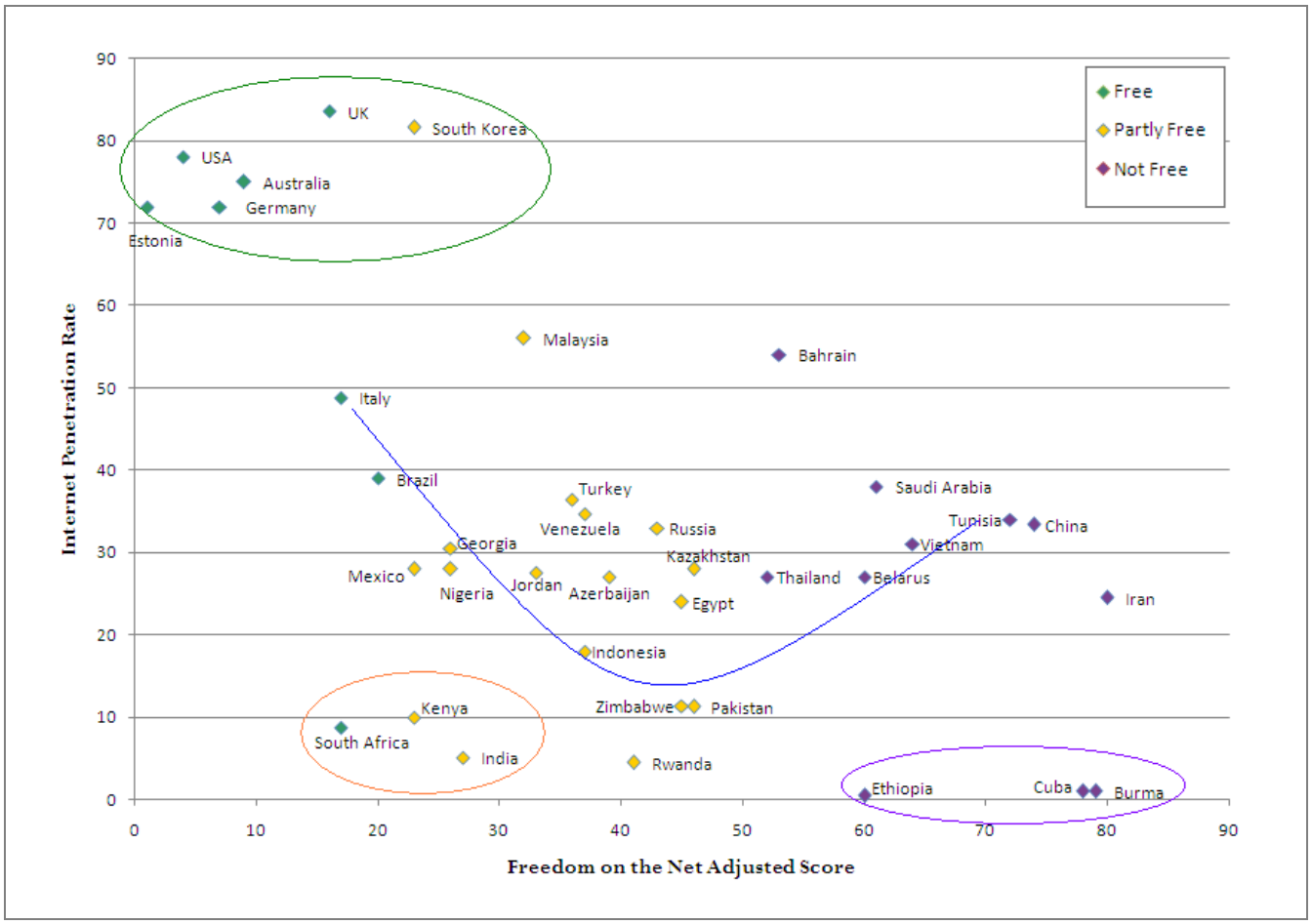


* The front-row bar reflects a country's *Freedom on the Net 2011* score; the back-row bar reflects the country's score on Freedom House's *Freedom of the Press* 2010 index, which primarily assesses television, radio, print media. A green-colored bar represents a status of **"Free,"** a yellow-colored bar represents a status of **"Partly Free,"** while a purple one, the status of **"Not Free."**

INTERNET FREEDOM VS. INTERNET PENETRATION

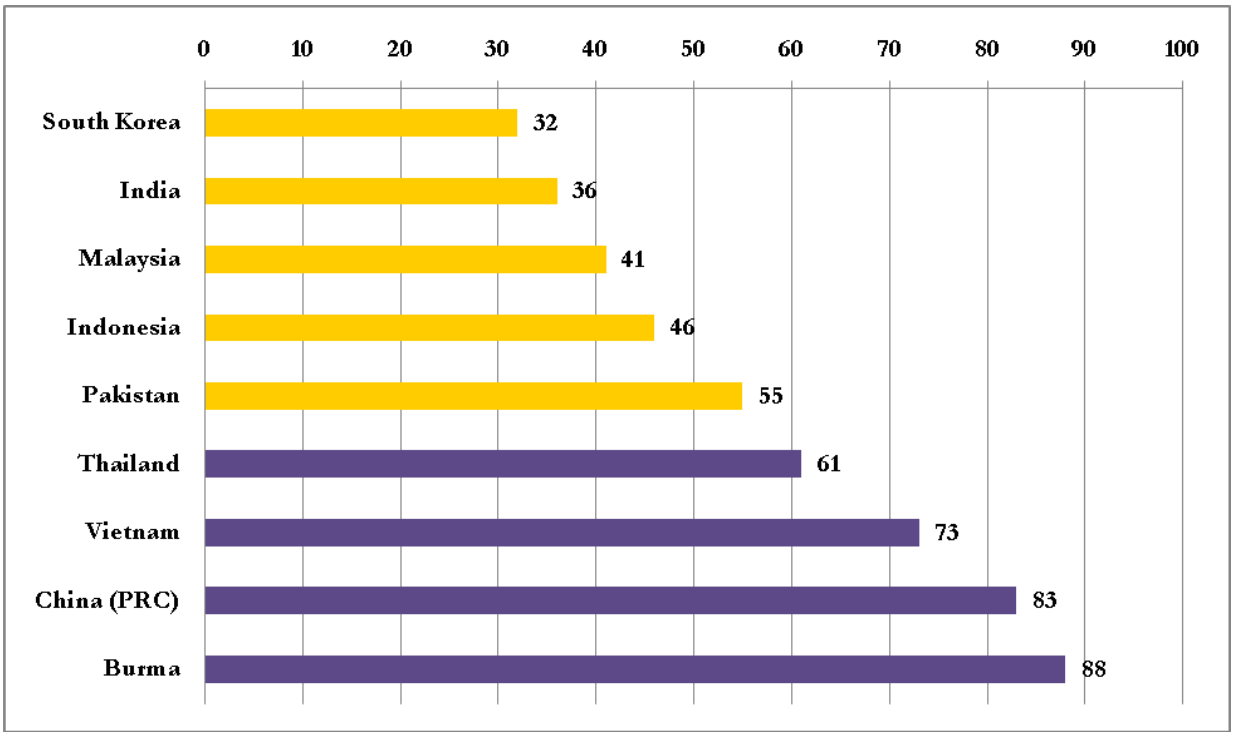
The figure below depicts the relationship between internet penetration rates and the level of digital media freedom as assessed by the *Freedom on the Net 2011* study. Each point is plotted to reflect its level of internet penetration as noted in the report, as well as its performance in the survey. To minimize possible overlap among variables, the scores have been adjusted to exclude performance on the first two questions of the *Freedom on the Net* methodology, which assess the degree of internet access in a given society.

The resulting graph points to several typologies: A cluster of economically developed democratic states with high penetration rates and relatively high levels of internet freedom **(green circle)**; A cluster of lower income democratic states, with relatively lower penetration rates but limited restrictions on other aspects of internet freedom **(orange circle)**; A cluster of lower income authoritarian states, with almost no internet access, as well as heavy restrictions on other aspects of internet freedom **(purple circle)**; A number of states with middling levels of internet penetration and a range of performance on internet freedom. Of note is a potential trajectory for the Partly Free countries in the middle, which may move towards greater repression (the high-tech, Not Free countries on the right) or better protection of free expression (the mid-penetration, Free countries on the left) as penetration rates increase **(blue V pattern)**.

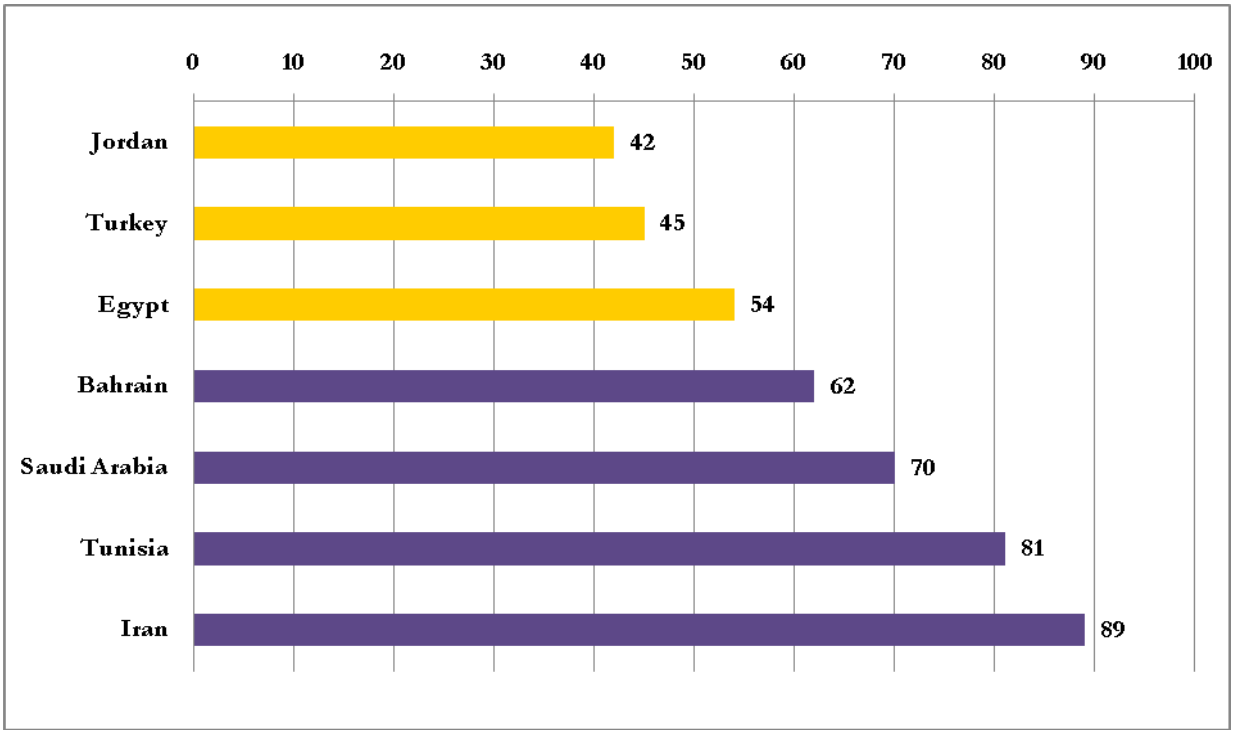


REGIONAL GRAPHS

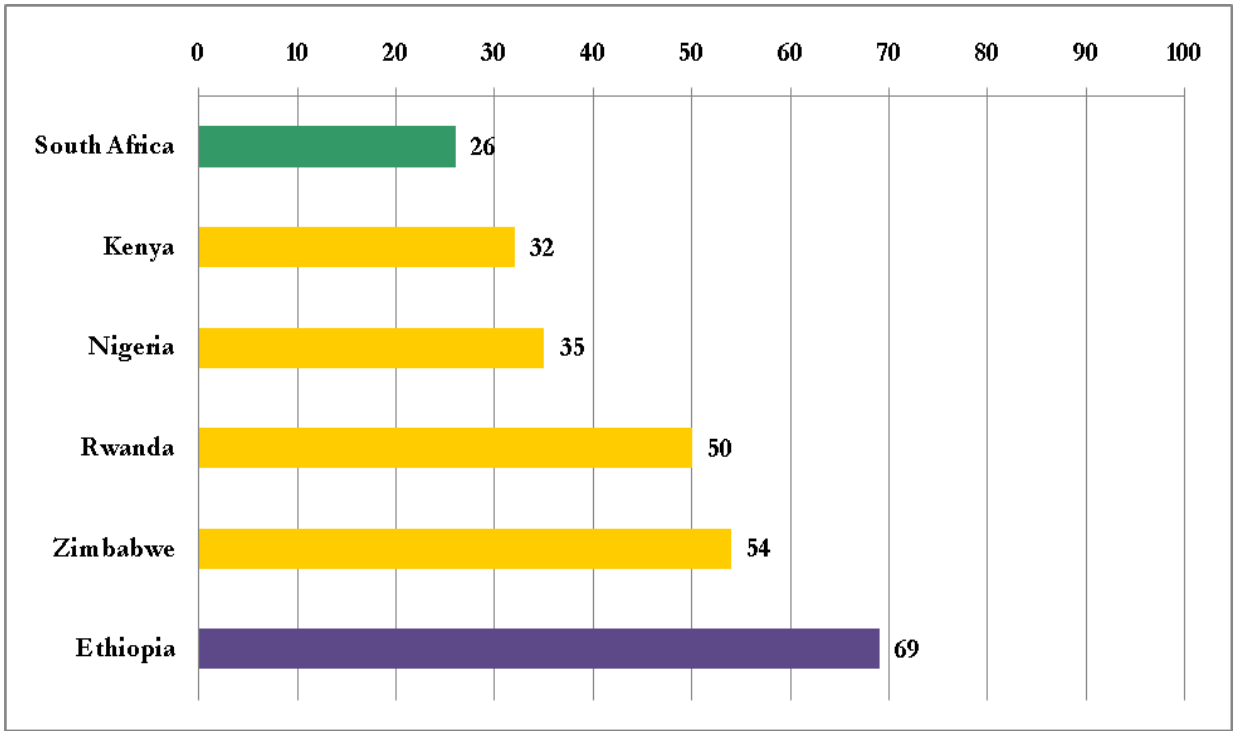
ASIA (0 best, 100 worst)



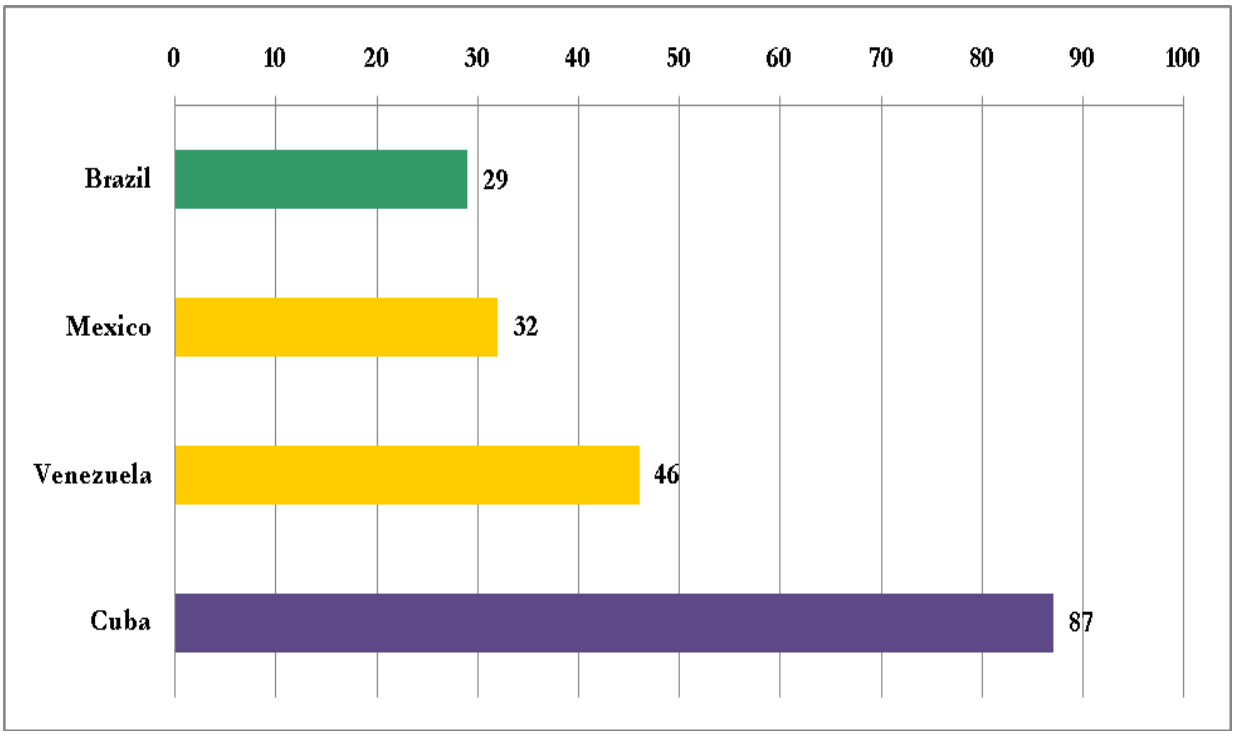
MIDDLE EAST & NORTH AFRICA (0 best, 100 worst)



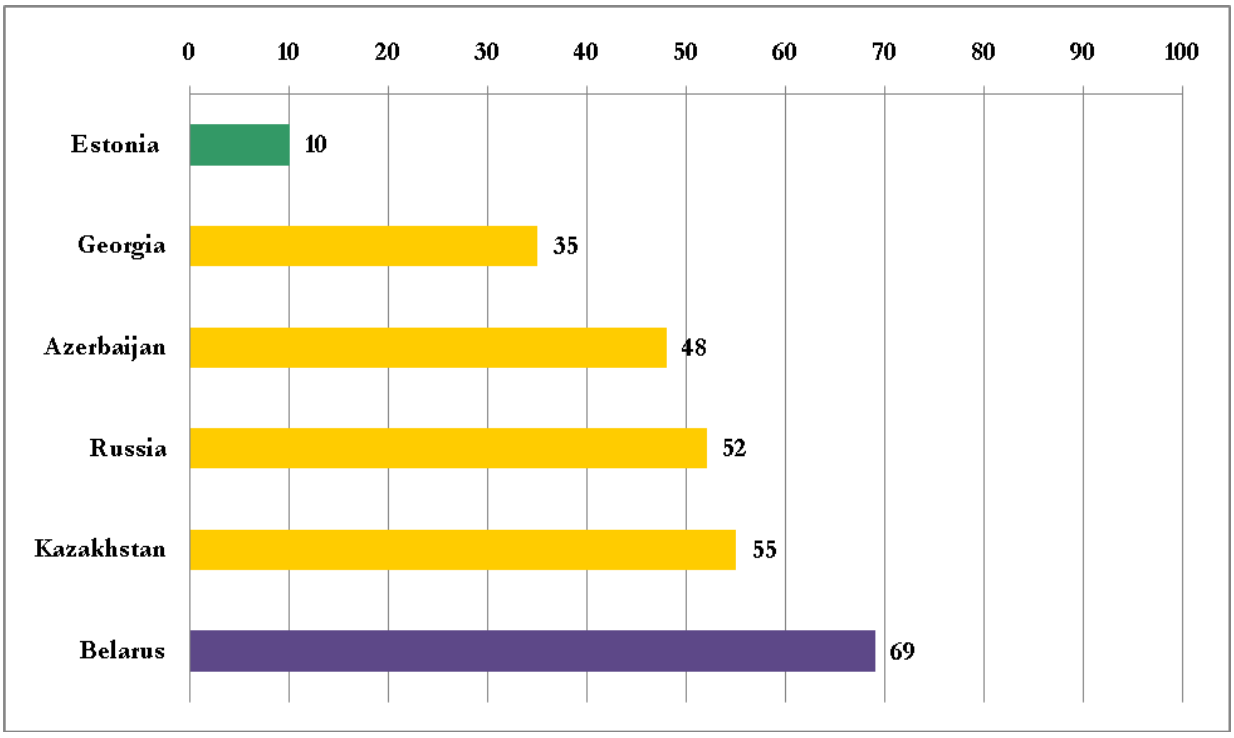
SUB-SAHARAN AFRICA (0 best, 100 worst)



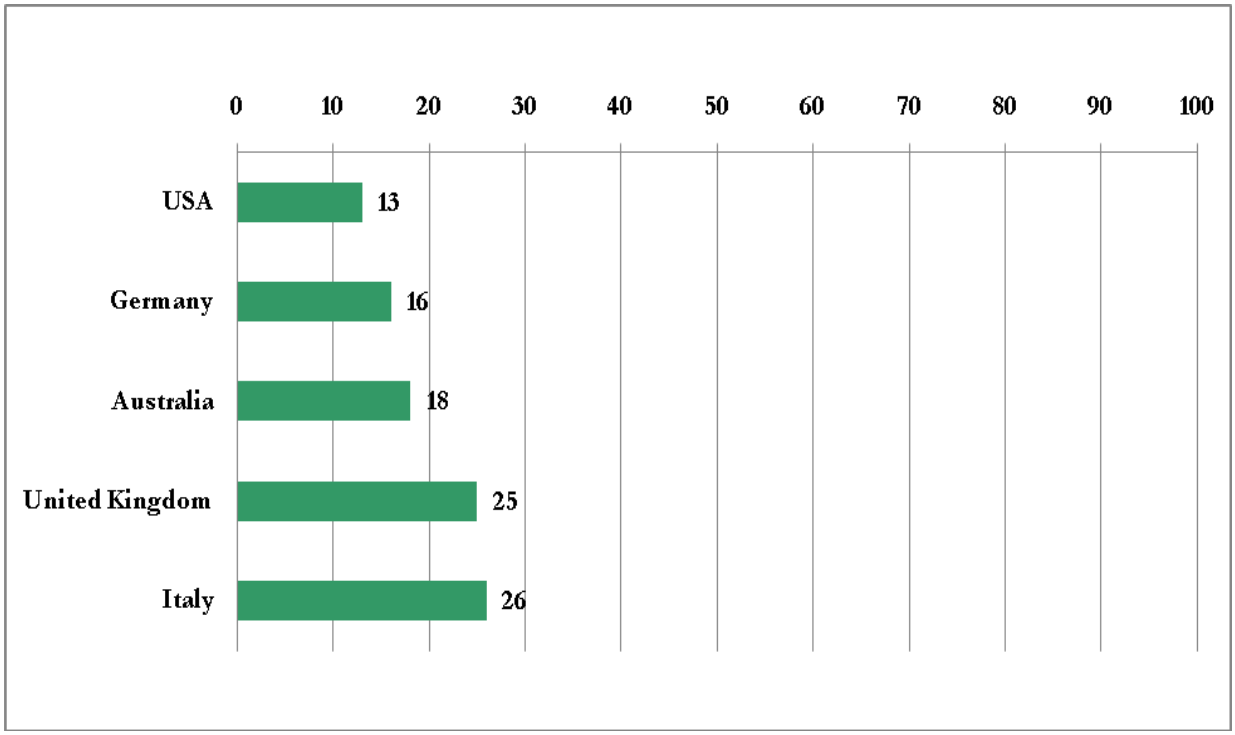
LATIN AMERICA (0 best, 100 worst)



FORMER SOVIET UNION (0 best, 100 worst)

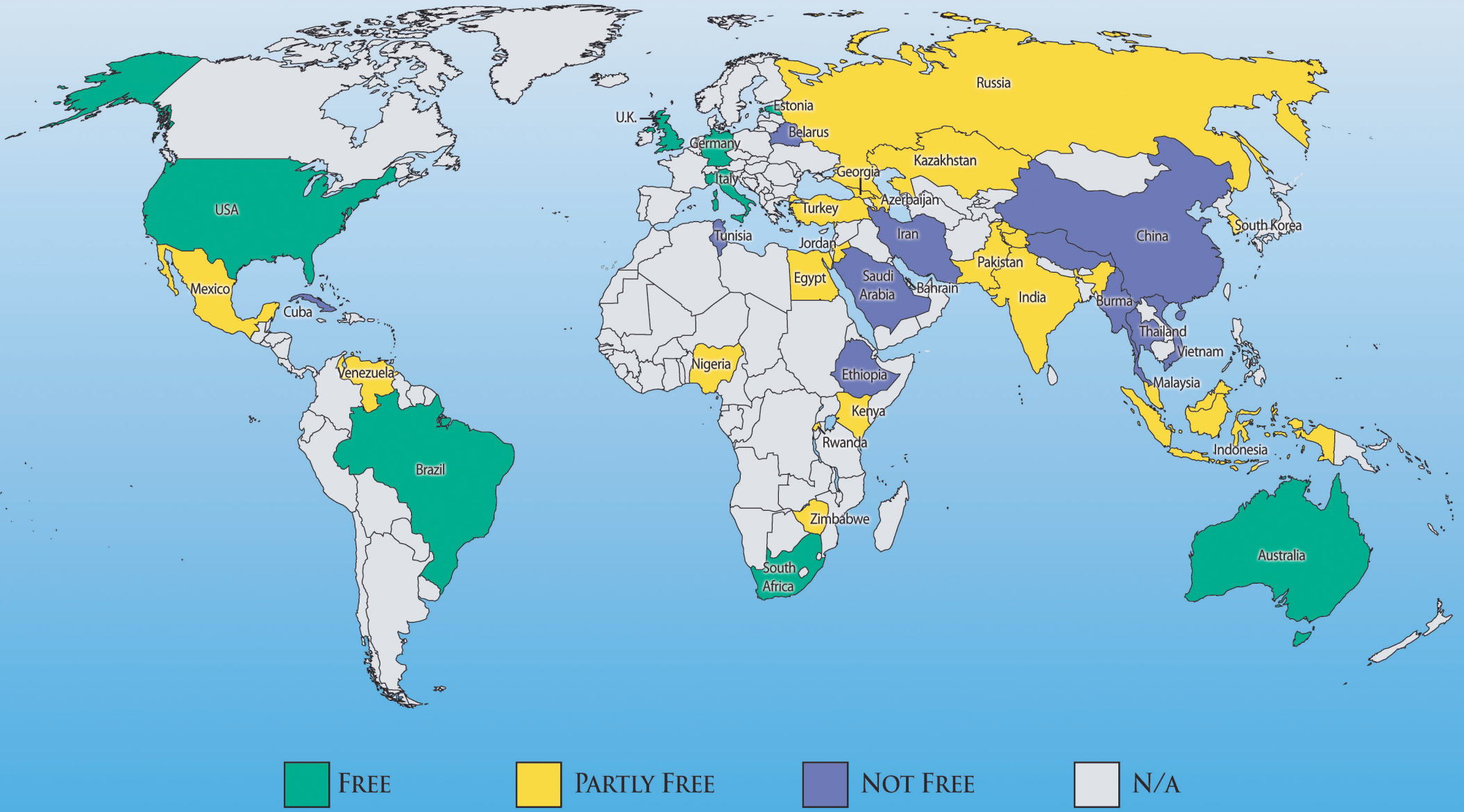


WESTERN EUROPE & OTHERS (0 best, 100 worst)



Freedom on the Net 2011

A Global Assessment of Internet and Digital Media



SCORE CHANGES AND EXPLANATIONS

Among the 37 countries covered in *Freedom on the Net 2011* are all 15 states that were assessed in the 2009 edition of the report. The following are explanations for score improvements and declines in this set of countries. For additional information, see individual Country Reports.

BRAZIL

Freedom on the Net 2009: 30 (Free)
Freedom on the Net 2011: 29 (Free)
Trajectory: Slight improvement

For a country with large social and economic disparities, Brazil has made significant gains in expanding internet access and mobile-phone usage. In recent years, access to the internet further improved, and the total number of users was the fourth largest in the world by 2009. Civic participation through internet media has correspondingly increased and restrictions on political campaigning via social-networking websites imposed ahead of the 2008 elections were removed for the run-up to the 2010 polls. Unlike in previous years, there were no instances of blocks on advanced web applications such as YouTube or the social-networking platform Orkut. These positive developments were slightly offset, however, by several legal and judicial actions that threatened free online expression, including cases of individual bloggers facing unreasonable defamation lawsuits, sometimes for very high amounts. Also noted was the impact of cyberattacks, as several prominent intelligence sources confirmed that a series of attacks in January 2005, September 2007, and November 2009 were responsible for blackouts.

CHINA

***Freedom on the Net 2009*: 79 (Not Free)
***Freedom on the Net 2011*: 83 (Not Free)
Trajectory: Notable decline

Although China is home to the world's largest population of internet users—numbering 446 million by the end of 2010—the country's internet environment remains one of the world's most restrictive, characterized by a sophisticated, multilayered control apparatus. In 2009 and 2010, this system was further enhanced, institutionalized, and decentralized. Blocks on international applications like Facebook and the Twitter became permanent, while censorship requirements on domestic alternatives were enhanced. The authorities also imposed a months-long shutdown of internet access in the western region of Xinjiang. By the end of 2010, the Chinese internet increasingly resembled an intranet. Many average users, isolated from international social media platforms and primarily exposed to a manipulated online information landscape, had limited knowledge of key events related to their own country, even when these make headlines around the world, a dynamic evident with the 2010 awarding of the Nobel Peace Prize to Chinese dissident Liu Xiaobo. In addition, the space for anonymous communication shrank and at least 70 people were in jail for internet-related reasons as of mid-2010, though the actual number of detainees is likely much higher. Tibetans, Uighurs, and Falun Gong practitioners are subject to especially harsh punishments for online activities, and two Uighurs were sentenced to life imprisonment. More than in previous years, China emerged as a key global source of cyberattacks, with targets ranging from groups reporting on Chinese human rights abuses to international financial, defense, and technology companies. The above restrictions were offset somewhat by the internet's continued growth as a primary source of news, a forum for discussion, and a mobilization channel

for many Chinese. Netizens successfully used it to challenge official misconduct, protest censorship, organize strikes, and obtain justice for ordinary citizens, while tech-savvy users employed circumvention tools to access banned sites, such as Twitter.

CUBA

***Freedom on the Net 2009*: 88 (Not Free)**
***Freedom on the Net 2011*: 87 (Not Free)**
Trajectory: Slight improvement

Cuba remains one of the world's most repressive environments for the internet and other information and communication technologies (ICTs). There is almost no access to internet applications other than e-mail, and surveillance is extensive, with special software employed to monitor and control many of the island's public internet-access points. Nevertheless, in recent years there has been a slight loosening of restrictions on the sale of computers, and important growth of mobile-phone infrastructure was evident in 2009. In addition, despite the threat of detention and travel restrictions, a community of bloggers has consolidated their work, creatively using online and offline means to express opinions and spread information about conditions in the country. Cuba still has the lowest mobile-phone penetration rate in Latin America, however, and most users continue to face extremely slow connections, making the use of multimedia applications nearly impossible.

EGYPT

***Freedom on the Net 2009*: 51 (Partly Free)**
***Freedom on the Net 2011*: 54 (Partly Free)**
Trajectory: Notable decline

While the Egyptian government has aggressively and successfully sought to expand access to the internet as an engine of economic growth, its security forces also intensified attempts to curtail the use of new technologies for disseminating and receiving sensitive political information in 2009 and 2010. They typically employ such "low-tech" methods as intimidation, legal harassment, detentions, and real-world surveillance of online dissidents. However, in response to increased internet-based activism, particularly in advance of the November 2010 parliamentary elections, the authorities began to engage in greater censorship of online communications. Several individuals who called for political change and democratic reform saw their websites shut down and two popular Facebook groups used for organizing protests were temporarily removed. With Emergency Law provisions in place, Egypt's legal environment remained harsh and several bloggers were detained during the coverage period, with one nearly tried before a military tribunal. In 2010, Egypt also saw the first court case in which a judge found a cybercafe owner liable for defamatory information posted online by a visitor to his shop.

ESTONIA

***Freedom on the Net 2009*: 13 (Free)**
***Freedom on the Net 2011*: 10 (Free)**
Trajectory: Notable improvement

Estonia ranks among the most wired and technologically advanced countries in the world. In 2009, over 91 percent of citizens filed their taxes online and Estonian identity cards were used to facilitate electronic voting during municipal and European Parliament elections. Restrictions on internet content and communications are among the lightest in the world. Nevertheless, in January 2010, a new law on online gambling came into force, requiring all domestic and foreign gambling sites to

obtain a special license or face access restrictions. The most serious threat to internet freedom in Estonia emerged in late April and early May 2007, when a campaign of cyberattacks targeted various Estonian institutions and infrastructures. Given the absence of such a large-scale attack in 2009-2010, and the subsequent restrictions it posed for access to important information, Estonia's score showed improvement during the coverage period. In addition, the experience led to increased awareness of the dangers of cyberattacks and a greater policy focus on improving technical competencies to make the internet more secure.

GEORGIA

***Freedom on the Net 2009*:** 43 (Partly Free)
***Freedom on the Net 2011*:** 35 (Partly Free)
Trajectory: Significant improvement

Use of the internet and related technologies has grown rapidly in Georgia in recent years, with internet penetration surpassing the 30 percent mark in 2009, partly the result of lower prices. There were no reports of government censorship during the coverage period and users were able to freely visit any website around the world, including advanced web applications. This was in contrast to the period in August 2008, during a brief military conflict with Russia, when the government blocked access to all Russian addresses (those using the .ru country code), including the popular blogging service LiveJournal. The filtering was eased within days and did not resurface. This change contributed to Georgia's score improvement, along with the absence of large-scale cyberattacks by Russian hackers that also featured in the 2008 conflict. Some restrictions on internet freedom did occur in 2009 and 2010, however. In November 2009, two young students were detained after allegedly insulting the widely respected head of the Georgian Orthodox Church in videos posted on YouTube. In addition, some online media outlets reported instances of advertisers deciding to withdraw ads after the outlet published news articles overly critical of the government.

INDIA

***Freedom on the Net 2009*:** 34 (Partly Free)
***Freedom on the Net 2011*:** 36 (Partly Free)
Trajectory: Slight decline

Although India's internet penetration rate of less than 10 percent is low by global standards, access has expanded rapidly in urban areas, generating tens of millions of new users in recent years. In the past, instances of the central government seeking to control communication technologies were relatively rare. However, following the November 2008 terrorist attacks in Mumbai and with an expanding Maoist insurgency, the need, desire, and ability of the Indian government to control the communications sector have grown. In 2008, Parliament passed amendments to the Information Technology Act (ITA), which came into effect in 2009 and have expanded the government's monitoring capabilities. Pressure has also increased on private intermediaries to remove certain information. Though most requests have targeted comments that might incite communal violence, some observers have raised concerns of certain removals being unnecessary. The fairness of bidding processes surrounding the allocation of ICT resources also came into question in 2010 with the exposure of a major corruption scandal involving the licensing of second-generation (2G) mobile-phone services.

IRAN

***Freedom on the Net 2009*: 76 (Not Free)**
***Freedom on the Net 2011*: 89 (Not Free)**
Trajectory: Significant decline

Iran showed the greatest decline among the countries surveyed, placing it as the worst performer in this edition. Since the protests that followed disputed presidential elections in June 2009, the Iranian authorities have waged an active campaign against internet freedom, employing extensive and sophisticated methods of control that go well beyond simple content filtering, though this too has become more severe since the election. Tactics employed include deliberately slowing internet speeds at critical times to make basic online activities difficult and ordering blogging service providers inside Iran to remove "offensive" posts. The regime has also sought to counter critical content and online organizing efforts by extending state propaganda into the digital sphere: over 400 news websites are either directly or indirectly supported by the state. Since June 2009, an increasing number of bloggers have been threatened, arrested, tortured, and kept in solitary confinement, and at least one blogger died in custody. Over 50 bloggers and online activists have been arrested, and a dozen remained in detention at the end of 2010. The Iranian authorities have taken a range of measures to monitor online communications, and a number of protesters who were put on trial after the election were indicted for their activities on Facebook and Balatarin, a Persian site that allows users to share links and news. A group calling itself the Iranian Cyber Army, later found to be associated with the Iranian authorities, also managed to hack a number of opposition and news sites with a mix of technical methods and forgery.

KENYA

***Freedom on the Net 2009*: 34 (Partly Free)**
***Freedom on the Net 2011*: 32 (Partly Free)**
Trajectory: Slight improvement

Although a lack of infrastructure and high costs still hamper connectivity for many Kenyans, the installation of two undersea cables in 2009 dramatically improved bandwidth to 13 times the speed from the previous year. Since 2008, there have been no confirmed incidents of government filtering or interference with online communication, despite earlier fears that the authorities might seek to impose greater controls after the internet was used as a channel for spreading hate speech during election-related violence. In January 2009, the government passed a controversial Communications Amendment Act, ignoring warnings from civil society that it could hinder free expression.

MALAYSIA

***Freedom on the Net 2009*: 41 (Partly Free)**
***Freedom on the Net 2011*: 41 (Partly Free)**
Trajectory: No change

By 2009, over 55 percent of the total population in Malaysia accessed the internet. In the watershed general elections of March 2008, the ruling National Front (BN) coalition lost its two-thirds parliamentary majority for the first time since 1969. The use of the internet for political mobilization and news dissemination was widely seen as contributing to the opposition's electoral gains. In both the run-up to and aftermath of the elections, many observers sensed that the government and ruling coalition had recognized the potential political impact of the internet and had therefore grown more determined to control it. Throughout 2009 and 2010, a number of bloggers faced legal harassment,

intimidation, fines, and brief periods of detention, though none were imprisoned. Many of these cases involve individuals who had been critical of Malaysian royalty, while others were detained over satirical content. The government also made a more concerted effort to influence public opinion by establishing its own presence online and several online news outlets and opposition-related websites faced cyberattacks. However, more systemic forms of censorship, such as technical filtering, were not implemented.

RUSSIA

***Freedom on the Net 2009*: 49 (Partly Free)**
***Freedom on the Net 2011*: 52 (Partly Free)**
Trajectory: Notable decline

With the tightening of traditional media controls since 2000, the internet has become Russia's last relatively uncensored platform for public debate. However, even as access conditions have improved, internet freedom has corroded. In the last two years, the country's first high-profile cases of technical blocking were reported, while tactics for proactively manipulating conversations in the online sphere were refined. Regional blocking, whereby a website is blocked in some areas but remains available elsewhere in the country, was particularly evident. In one example of the phenomenon, a regional network provider in December 2010 temporarily blocked users from accessing an environmentalist website, allegedly because the site initiated a petition to dismiss a local mayor. Russian bloggers also faced increasing intimidation: at least 25 cases of blogger harassment by the authorities occurred in 2009 and 2010, including 11 arrests. In addition, several newspaper websites experienced cyberattacks, typically in connection with articles that could seriously influence offline events. At least 16 blogs suffered hacking attacks during the coverage period.

SOUTH AFRICA

***Freedom on the Net 2009*: 24 (Free)**
***Freedom on the Net 2011*: 26 (Free)**
Trajectory: Slight decline

Digital media freedom continues to be respected in South Africa. Access to the internet has improved, with more people having an option to access the internet from their mobile telephones than from computers, though the majority of the population is unable to benefit from internet access. While internet content remains largely free of government censorship, a recent amendment to the Films and Publications Act of 1996 has raised fears that controversial content could be restricted. The amendment, which was passed into law in 2009, requires that every print and online publication that is not a recognized newspaper be submitted for classification to the government-controlled Film and Publications Board if it includes depictions of sexual or disrespectful content. Other areas of concern include lack of parliamentary oversight in relation to interception orders and lack of transparency surrounding take-down notices, though there were no known instances of such requests targeting politically relevant content.

TUNISIA

***Freedom on the Net 2009*: 76 (Not Free)**
***Freedom on the Net 2011*: 81 (Not Free)**
Trajectory: Notable decline

Since the government tightly controls traditional media, the internet has emerged as a comparatively open forum for airing political and social opinions. As internet penetration grew, reaching 34 percent of the population by 2009, the regime of former President Ben Ali

responded by creating a multilayered censorship apparatus that was among the world's most sophisticated. Despite an already robust system in place, in 2009 and especially in 2010, censorship expanded and became increasingly arbitrary. Several human rights activists and online journalists were arbitrarily detained, monitored and harassed, while websites were subject to targeted technical attacks, sometimes causing deletion of large amounts of content. Conditions further deteriorated after an unemployed fruit vendor set himself on fire in later December 2010 to protest joblessness, sparking country-wide protests, along with calls for political reform and greater employment opportunities. Social media sites such as Twitter, YouTube, and Facebook, as well as various blogs, played an important role in providing independent information and analysis, spreading the protesters' demands, and showing videos of demonstrations across the country. This, in turn, resulted in the government's increased efforts to dismantle networks of online activists, hack into their social networking and blogging accounts, conduct extensive online surveillance, and disable activists' online profiles and blogs.

TURKEY

***Freedom on the Net 2009*: 42 (Partly Free)**
***Freedom on the Net 2011*: 45 (Partly Free)**
Trajectory: Notable decline

Internet and mobile-telephone use in Turkey has grown significantly in recent years, surpassing one third of the population in 2009, though access remains a challenge in some parts of the country. Since 2001, the government has taken considerable legal steps to limit access to certain information, including some political content. According to various estimates, there were over 5,000 blocked websites as of July 2010, an increase from 2008, spurring street demonstrations against internet censorship. In addition, certain applications, particularly file-sharing sites like YouTube, Last.fm, and Metacafe, as well as some Google-related services, have been repeatedly blocked. The YouTube block was eventually lifted in November 2010, but only after disputed videos were removed or made unavailable within the country. Despite a restrictive legal environment, the Turkish blogosphere is vibrant and diverse. Bloggers have critiqued even sensitive government policies and sought to raise public awareness about censorship and surveillance practices, yielding at least one parliamentary inquiry into the latter.

UNITED KINGDOM

***Freedom on the Net 2009*: 23 (Free)**
***Freedom on the Net 2011*: 25 (Free)**
Trajectory: Slight decline

The United Kingdom has high levels of internet penetration, and online free expression is generally respected. However, both the government and private parties have presented challenges to free speech in connection with antiterrorism efforts, public order, and intellectual property. The biggest recent controversy was the adoption of the Digital Economy Act in April 2010. The law allows for the blocking of websites and the cutting off of user accounts based on claims of intellectual-property rights violations. Free expression advocates also complain that procedures for blocking and removing content related to pornography and terrorism are not transparent, clear, or supported by an adequate appeals process. In efforts to combat terrorism, the government has taken measures against users who post or download information perceived as a security threat, including one case of a man convicted for using Twitter to express dismay at the closing of a local airport and writing that he would blow up the airport if it did not reopen within a week. The newly elected coalition government has promised to review and repeal a number of laws that negatively affect online rights, including expansively interpreted libel laws.

METHODOLOGY

This second edition of *Freedom on the Net* provides analytical reports and numerical ratings for 37 countries worldwide. The countries were chosen to provide a representative sample with regards to geographical diversity and economic development, as well as varying levels of political and media freedom. The ratings and reports included in this study particularly focus on developments that took place between January 1, 2009 and December 31, 2010.

WHAT WE MEASURE

The *Freedom on the Net* index aims to measure each country's level of internet and digital media freedom based on a set of methodology questions described below (see "Checklist of Questions"). Given increasing technological convergence, the index also measures access and openness of other digital means of transmitting information, particularly mobile phones and text messaging services.

Freedom House does not maintain a culture-bound view of freedom. The project methodology is grounded in basic standards of free expression, derived in large measure from Article 19 of the Universal Declaration of Human Rights:

> *"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive, and impart information and ideas through any media regardless of frontiers."*

This standard applies to all countries and territories, irrespective of geographical location, ethnic or religious composition, or level of economic development.

The project particularly focuses on the transmission and exchange of news and other politically relevant communications, as well as the protection of users' rights to privacy and freedom from both legal and extralegal repercussions arising from their online activities. At the same time, the index acknowledges that in some instances freedom of expression and access to information may be legitimately restricted. The standard for such restrictions applied in this index is that they be implemented only in narrowly defined circumstances and in line with international human rights standards, the rule of law, and the principles of necessity and proportionality. As much as possible, censorship and surveillance policies and procedures should be transparent and include avenues for appeal available to those affected.

The index does not rate governments or government performance per se, but rather the real-world rights and freedoms enjoyed by individuals within each country. While digital

media freedom may be primarily affected by state actions, pressures and attacks by nonstate actors, including the criminal underworld, are also considered. Thus, the index ratings generally reflect the interplay of a variety of actors, both governmental and nongovernmental, including private corporations.

THE SCORING PROCESS

The index aims to capture the entire "enabling environment" for internet freedom within each country through a set of 21 methodology questions, divided into three subcategories, which are intended to highlight the vast array of relevant issues. Each individual question is scored on a varying range of points. Assigning numerical points allows for comparative analysis among the countries surveyed and facilitates an examination of trends over time. Countries are given a total score from 0 (best) to 100 (worst) as well as a score for each subcategory. Countries scoring between 0 to 30 points overall are regarded as having a "Free" internet and digital media environment; 31 to 60, "Partly Free"; and 61 to 100, "Not Free". An accompanying country report provides narrative detail on the points covered by the methodology questions.

The methodology examines the level of internet freedom through a set of 21 questions and nearly 100 accompanying subpoints, organized into three groupings:

- ***Obstacles to Access***—including infrastructural and economic barriers to access; governmental efforts to block specific applications or technologies; legal and ownership control over internet and mobile phone access providers.
- ***Limits on Content***—including filtering and blocking of websites; other forms of censorship and self-censorship; manipulation of content; the diversity of online news media; and usage of digital media for social and political activism.
- ***Violations of User Rights***—including legal protections and restrictions on online activity; surveillance and limits on privacy; and repercussions for online activity, such as legal prosecution, imprisonment, physical attacks, or other forms of harassment.

The purpose of the subpoints is to guide analysts regarding factors they should consider while evaluating and assigning the score for each methodology question. After researchers submitted their draft scores, Freedom House convened three regional review meetings and several international conference calls, attended by Freedom House staff and a range of local experts, scholars, and civil society representatives from the countries under study. During the meetings, participants reviewed, critiqued, and adjusted the draft scores through careful consideration of events, laws, and practices relevant to each item. After

completing the regional and country consultations, Freedom House staff did a final review of all scores to ensure their comparative reliability and integrity.

**** Note on changes from 2009 pilot edition***

Freedom House released a pilot edition of *Freedom on the Net* in April 2009, assessing a sample of 15 countries. Following the report's publication and drawing on feedback from a range of audiences, including analysts and academic advisers involved in production of the pilot study, Freedom House staff made several modifications to the methodology. In particular, question B1 on censorship and question C7 on attacks were each split into two separate questions in order to clarify and sharpen the analytical rigor with which obstacles to internet freedom are identified. In addition, in order to retain the accuracy of score comparisons between the pilot edition and this study, for those countries included in both, a number of minor adjustments were made to the 2009 scores on the basis of updated scoring guidelines used for the 2011 edition. In the present edition, the adjusted 2009 scores are presented in order to best convey changes over time in each country assessed.

CHECKLIST OF QUESTIONS

- Each country is ranked on a scale of 0 to 100, with 0 being the best and 100 being the worst.
- A combined score of 0-30=Free, 31-60=Partly Free, 61-100=Not Free.
- Under each question, **a lower number of points is allotted for a more free situation, while a higher number of points is allotted for a less free environment.**
- Unless otherwise indicated, the sub-questions listed are meant to provide guidance as to what Issues should be addressed under each methodology question, though not all will apply to every country.

A. OBSTACLES TO ACCESS (0-25 POINTS)

1. **To what extent do infrastructural limitations restrict access to the internet and other ICTs? (0-6 points)**
   - *Does poor infrastructure (electricity, telecommunications, etc) limit citizens' ability to receive internet in their homes and businesses?*
   - *To what extent is there widespread public access to the internet through internet cafes, libraries, schools and other venues?*
   - *To what extent is there internet and mobile phone access, including via 3G networks or satellite?*
   - *Is there a significant difference between internet and mobile-phone penetration and access in rural versus urban areas or across other geographical divisions?*
   - *To what extent are broadband services widely available in addition to dial-up?*

2. **Is access to the internet and other ICTs prohibitively expensive or beyond the reach of certain segments of the population? (0-3 points)**
   - *In countries where the state sets the price of internet access, is it prohibitively high?*
   - *Do financial constraints, such as high costs of telephone/internet services or excessive taxes imposed on such services, make internet access prohibitively expensive for large segments of the population?*
   - *Do low literacy rates (linguistic and "computer literacy") limit citizens' ability to use the internet?*
   - *Is there a significant difference between internet penetration and access across ethnic or socio-economic societal divisions?*
   - *To what extent are online software, news, and other information available in the main local languages spoken in the country?*

3. **Does the government impose restrictions on ICT connectivity and access to particular Web 2.0 applications permanently or during specific events? (0-6 points)**
   - *Does the government place limits on the amount of bandwidth that access providers can supply?*
   - *Does the government use control over internet infrastructure (routers, switches, etc.) to limit connectivity, permanently or during specific events?*
   - *Does the government centralize telecommunications infrastructure in a manner that could facilitate control of content and surveillance?*
   - *Does the government block protocols and tools that allow for instant, person-to-person communication (VOIP, instant messaging, text messaging, etc.), particularly those based outside the country (i.e. YouTube, Facebook, Skype, etc.)?*
   - *Does the government block protocols and Web 2.0 applications that allow for information sharing or building online communities (video-sharing, social-networking sites, comment features, blogging platforms, etc.) permanently or during specific events?*
   - *Is there blocking of certain tools that enable circumvention of online filters and censors?*

4. **Are there legal, regulatory, or economic obstacles that prevent the existence of diverse business entities providing access to digital technologies? (0-6 points)**

   Note: Each of the following access providers are scored separately:

   1a. Internet-service providers (ISPs) and other backbone internet providers (0-2 points)
   1b. Cybercafes and other businesses that allow public internet access (0-2 points)
   1c. Mobile phone companies (0-2 points)

   - *Is there a legal or de facto monopoly over access providers or do users have a choice of access provider, including ones privately owned?*
   - *Is it legally possible to establish a private access provider or does the state place extensive legal or regulatory controls over the establishment of providers?*
   - *Are registration requirements (e.g. bureaucratic "red tape") for establishing an access provider unduly onerous or are they approved/rejected on partisan or prejudicial grounds?*
   - *Does the state place prohibitively high fees on the establishment and operation of access providers?*

5. **To what extent do national regulatory bodies overseeing digital technology operate in a free, fair, and independent manner? (0-4 points)**
   - *Are there explicit legal guarantees protecting the independence and autonomy of any regulatory body overseeing internet and other ICTs (exclusively or as part of a broader mandate) from political or commercial interference?*
   - *Is the process for appointing members of regulatory bodies transparent and representative of different stakeholders' interests?*
   - *Are decisions taken by the regulatory body, particularly those relating to ICTs, seen to be fair and apolitical and to take meaningful notice of comments from stakeholders in society?*

- *Are efforts by access providers and other internet-related organizations to establish self-regulatory mechanisms permitted and encouraged?*
- *Does the allocation of digital resources, such as domain names or IP addresses, on a national level by a government-controlled body create an obstacle to access or are they allocated in a discriminatory manner?*

B. LIMITS ON CONTENT (0-35 POINTS)

1. **To what extent does the state or other actors block or filter internet and other ICT content, particularly on political and social issues? (0-6 points)**
   - *Is there significant blocking or filtering of internet sites, web pages, blogs, or data centers, particularly those related to political and social topics?*
   - *Is there significant filtering of text messages or other content transmitted via mobile phones?*
   - *Do state authorities block or filter information and views from inside the country—particularly concerning human rights abuses, government corruption, and poor standards of living—from reaching the outside world through interception of e-mail or text messages, etc?*
   - *Are methods such as deep-packet inspection used for the purposes of preventing users from accessing certain content or for altering the content of communications en route to the recipient, particularly with regards to political and social topics?*

2. **To what extent does the state employ legal, administrative, or other means to force deletion of particular content, including requiring private access providers to do so? (0-4 points)**
   - *To what extent are non-technical measures—judicial or extra-legal—used to order the deletion of content from the internet, either prior to or after its publication?*
   - *To what degree does the government or other powerful political actors pressure or coerce online news outlets to exclude certain information from their reporting?*
   - *Are access providers and content hosts legally responsible for the information transmitted via the technology they supply or required to censor the content accessed or transmitted by their users?*
   - *Are access providers or content hosts prosecuted for opinions expressed by third parties via the technology they supply?*

3. **To what extent are restrictions on internet and ICT content transparent, proportional to the stated aims, and accompanied by an independent appeals process? (0-4 points)**
   - *Are there national laws, independent oversight bodies, and other democratically accountable procedures in place to ensure that decisions to restrict access to certain content are proportional to their stated aim?*
   - *Are state authorities transparent about what content is blocked or deleted (both at the level of public policy and at the moment the censorship occurs)?*
   - *Do state authorities block more types of content than they publicly declare?*

- *Do independent avenues of appeal exist for those who find content they produced to have been subjected to censorship?*

4. Do online journalists, commentators, and ordinary users practice self-censorship? (0-4 points)

- *Is there widespread self-censorship by online journalists, commentators, and ordinary users in state-run online media, privately run websites, or social media applications?*
- *Are there unspoken "rules" that prevent an online journalist or user from expressing certain opinions in ICT communication?*
- *Is there avoidance of subjects that can clearly lead to harm to the author or result in almost certain censorship?*

5. To what extent is the content of online sources of information determined or manipulated by the government or a particular partisan interest? (0-4 points)

- *To what degree do the government or other powerful actors pressure or coerce online news outlets to follow a particular editorial direction in their reporting?*
- *Do authorities issue official guidelines or directives on coverage to online media outlets, blogs, etc., including instructions to marginalize or amplify certain comments or topics for discussion?*
- *Do government officials or other actors bribe or use close economic ties with online journalists, bloggers, website owners, or service providers in order to influence the online content they produce or host?*
- *Does the government employ, or encourage content providers to employ, individuals to post pro-government remarks in online bulletin boards and chat rooms?*
- *Do online versions of state-run or partisan traditional media outlets dominate the online news landscape?*

6. Are there economic constraints that negatively impact users' ability to publish content online or online media outlets' ability to remain financially sustainable? (0-3 points)

- *Are favorable connections with government officials necessary for online media outlets or service providers (e.g. search engines, e-mail applications, blog hosting platforms, etc.) to be economically viable?*
- *Are service providers who refuse to follow state-imposed directives to restrict content subject to sanctions that negatively impact their financial viability?*
- *Does the state limit the ability of online media to accept advertising or investment, particularly from foreign sources, or does it limit advertisers from conducting business with disfavored online media or service providers?*
- *To what extent do ISPs manage network traffic and bandwidth availability to users in a manner that is transparent, evenly applied, and does not discriminate against users or producers of content based on the content/source of the communication itself (i.e. respect "net neutrality" with regard to content)?*
- *To what extent do users have access to free or low-costs blogging services, webhosts, etc. to allow them to make use of the internet to express their own views?*

7. **To what extent are sources of information that are robust and reflect a diversity of viewpoints readily available to citizens, despite government efforts to limit access to certain content? (0-4 points)**
   - *Are people able to access a range of local and international news sources via the internet or text messages, despite efforts to restrict the flow of information?*
   - *Does the public have ready access to media outlets or websites that express independent, balanced views?*
   - *Does the public have ready access to sources of information that represent a range of political and social viewpoints?*
   - *To what extent do online media outlets and blogs represent diverse interests within society, for example through websites run by community organizations or religious, ethnic and other minorities?*
   - *To what extent do users employ proxy servers and other methods to circumvent state censorship efforts?*

8. **To what extent do individuals use the internet and other ICT technologies as sources of information and tools for mobilization, particularly regarding political and social issues? (0-6 points)**
   - *Are internet sources (news websites, blogs, etc) a primary medium of news dissemination for a large percentage of the population?*
   - *To what extent does the online community cover political developments and provide scrutiny of government policies, official corruption, or actions by other powerful societal actors?*
   - *To what extent are online communication (e.g. Twitter) or social networking sites (e.g. Facebook, Orkut) used as a means to organize politically, including for "real-life" activities?*
   - *Are cell phones and ICTs used as a medium of news dissemination and political organization, including on otherwise banned topics?*

C. VIOLATIONS OF USER RIGHTS (0-40 POINTS)

1. **To what extent does the constitution or other laws contain provisions designed to protect freedom of expression, including on the internet, and are they enforced? (0-6 points)**
   - *Does the constitution contain language that provides for freedom of speech and of the press generally?*
   - *Are there laws or legal decisions that specifically protect online modes of expression?*
   - *Are online journalists and bloggers accorded the same rights and protections given to print and broadcast journalists?*
   - *Is the judiciary independent and do the Supreme Court, Attorney General, and other representatives of the higher judiciary support free expression?*
   - *Is there implicit impunity for private and/or state actors who commit crimes against online journalists, bloggers, or other citizens targeted for their online activities?*

2. **Are there laws which call for criminal penalties or civil liability for online and ICT activities? (0-4 points)**
   - *Are there specific laws criminalizing online expression and activity such as posting or downloading information, sending an e-mail, or text message, etc.? (Note: this excludes legislation addressing harmful content such as child pornography or activities such as malicious hacking)*
   - *Do laws restrict the type of material that can be communicated in online expression or via text messages, such as communications about ethnic or religious issues, national security, or other sensitive topics?*
   - *Are restrictions of internet freedom closely defined, narrowly circumscribed, and proportional to the legitimate aim?*
   - *Are vaguely worded penal codes or security laws applied to internet-related or ICT activities?*
   - *Are there penalties for libeling officials or the state in online content?*
   - *Can an online outlet based in another country be sued if its content can be accessed from within the country (i.e. "libel tourism")?*

3. **Are individuals detained, prosecuted or sanctioned by law enforcement agencies for disseminating or accessing information on the internet or via other ICTs, particularly on political and social issues? (0-6 points)**
   - *Are writers, commentators, or bloggers subject to imprisonment or other legal sanction as a result of posting material on the internet?*
   - *Are citizens subject to imprisonment, civil liability, or other legal sanction as a result of accessing or downloading material from the internet or for transmitting information via e-mail or text messages?*
   - *Does the lack of an independent judiciary or other limitations on adherence to the rule of law hinder fair proceedings in ICT-related cases?*
   - *Are individuals subject to abduction or arbitrary detention as a result of online activities, including membership in certain online communities?*
   - *Are penalties for "irresponsible journalism" or "rumor mongering" applied widely?*
   - *Are online journalists, bloggers, or others regularly prosecuted, jailed, or fined for libel or defamation (including in cases of "libel tourism")?*

4. **Does the government place restrictions on anonymous communication or require user registration? (0-4 points)**
   - *Are website owners, bloggers, or users in general required to register with the government?*
   - *Are users able to post comments online or purchase mobile phones anonymously or does the government require that they use their real names or register with the government?*
   - *Are users prohibited from using encryption software to protect their communications?*
   - *Are there laws restricting the use of encryption and other security tools, or requiring that the government be given access to encryption keys and algorithms?*

5. **To what extent is there state surveillance of internet and ICT activities without judicial or other independent oversight, including systematic retention of user traffic data? (0-6 points)**
   - *Do the authorities regularly monitor websites, blogs, and chat rooms, or the content of e-mail and mobile text messages, including via deep-packet inspection?*
   - *To what extent are restrictions on the privacy of digital media users transparent, proportional to the stated aims, and accompanied by an independent process for lodging complaints of violations?*
   - *Where the judiciary is independent, are there procedures in place for judicial oversight of surveillance and to what extent are these followed?*
   - *Where the judiciary lacks independence, is there another independent oversight body in place to guard against abusive use of surveillance technology and to what extent is it able to carry out its responsibilities free of government interference?*
   - *Is content intercepted during internet surveillance admissible in court or has it been used to convict users in cases involving free speech?*

6. **To what extent are providers of access to digital technologies required to aid the government in monitoring the communications of their users? (0-6 points)**

   Note: Each of the following access providers are scored separately:

   1a. Internet-service providers (ISPs) and other backbone internet providers (0-2 points)
   1b. Cybercafes and other businesses that allow public internet access (0-2 points)
   1c. Mobile phone companies (0-2 points)

   - *Are access providers required to monitor their users and supply information about their digital activities to the government (either through technical interception or via manual monitoring, such as user registration in cybercafes)?*
   - *Are access providers prosecuted for not doing so?*
   - *Does the state attempt to control access providers through less formal methods, such as codes of conduct?*
   - *Can the government obtain information about users without a legal process?*

7. **Are bloggers, other ICT users, websites, or their property subject to extralegal intimidation or physical violence by state authorities or any other actor? (0–5 points)**
   - *Are individuals subject to murder, beatings, harassment, threats, travel restrictions, or torture as a result of online activities, including membership in certain online communities?*
   - *Do armed militias, organized crime elements, insurgent groups, political or religious extremists, or other organizations regularly target online commentators?*
   - *Have online journalists, bloggers, or others fled the country or gone into hiding to avoid such action?*
   - *Have cybercafes or property of online commentators been targets of physical attacks or the confiscation or destruction of property as retribution for online activities or expression?*

8. **Are websites, governmental and private entities, ICT users, or service providers subject to widespread "technical violence," including cyberattacks, hacking, and other malicious threats? (0-3 points)**
   - *Are financial, commercial, and governmental entities subject to significant and targeted cyberattacks (e.g. cyber espionage, data gathering, DoS attacks), including those originating from outside of the country?*
   - *Have websites belonging to opposition or civil society groups within the country's boundaries been temporarily or permanently disabled due to cyberattacks, particularly at politically sensitive times?*
   - *Are websites or blogs subject to targeted technical attacks as retribution for posting certain content (e.g. on political and social topics)?*
   - *Are laws and policies in place to prevent and protect against cyberattacks (including the launching of systematic attacks by non-state actors from within the country's borders) and are they enforced?*

ACKNOWLEDGMENTS

Completion of the *Freedom on the Net* publication would not have been possible without the tireless efforts of the following people.

As managing editor, Sanja Kelly directed the research, editorial, and administrative operations for the project, supported by Asia research analyst and assistant editor Sarah Cook. Together, they provided essential research and analysis, edited the country reports, and conducted field visits in Turkey, Malaysia, and South Africa. Over 40 external consultants served as report authors and advisors, and made an outstanding contribution by producing informed analyses of a highly diverse group of countries and complex set of issues. Tyler Roylance copyedited the volume and provided critical editorial and analytical insight throughout. Interns Abha Parekh and Sabrina Baum provided indispensable research, editorial, and administrative assistance.

General oversight was provided by Christopher Walker, director of studies. Helpful contributions and insights were made by Daniel Calingaert, deputy director of programs, Robert Guerra, internet freedom project director, as well as other Freedom House staff in the United States and abroad including Jake Dizard, Karin Karlekar, Rashweat Mukundu, Matthew Brady, Viviana Giacaman, Sherif Mansour, Miwa Kubosaki, Piet Khaidir, Julie Middleton, and Kerryn Shewitz. Experts from the Center for Democracy and Technology—Leslie Harris, Jim Dempsey, and Cynthia Wong—also provided valuable feedback.

This publication was produced with the generous assistance of the United Nations Democracy Fund (UNDEF) and Google. Additional contributions were also made by the Dutch Ministry of Foreign Affairs and the United States Agency for International Development (USAID). The content of the publication is the sole responsibility of Freedom House and does not necessarily reflect the views of the United Nations, UNDEF or its Advisory Board, Google, the Dutch Ministry, USAID, or any other funder.

CONTRIBUTORS

FREEDOM HOUSE STAFF

- Sanja Kelly, Senior Researcher and Managing Editor, Freedom House
- Sarah Cook, Asia Analyst and Assistant Editor, Freedom House

REPORT AUTHORS AND ADVISORS

- **Australia:** Alana Maurushat, Academic Director, Cyberspace Law and Policy Centre, University of New South Wales
- **Brazil:** Carolina Rossini, attorney and coordinator for the Brazilian Open Educational Resources Project
- **Burma**: Min Zin, Burmese journalist and graduate student in political science at the University of California, Berkeley
- **China** (Advisor)**:** Xiao Qiang, Director of China Internet Project and an adjunct professor, Graduate School of Journalism, University of California, Berkeley
- **Cuba:** Ernesto Hernández Busto, blogger and journalist based in Spain
- **Estonia:** Linnar Viik, information society expert and Rector, Estonian IT College
- **Georgia:** Giorgi (Giga) Paitchadze, founder of Georgian New Media Institute
- **Germany:** Heike Jensen, lecturer at the Department of Gender Studies of Humboldt University, Berlin
- **India:** Ketan Tanna, Feature and Web Editor, *The Free Press Journal*, Mumbai
- **Iran:** Mahmood Enayat, Director, Iran Media Program, Annenberg School of Communication, University of Pennsylvania
- **Italy:** Giampiero Giacomello, Assistant Professor of International Relations, University of Bologna
- **Jordan:** Sa'eda Kilani, Founder and General Director, Arab Archives Institute, Amman

- **Kazakhstan**: Yelena Jetpyspayeva, consultant and Managing Editor, NewEurasia.net
- **Kenya:** Ory Okolloh, lawyer, blogger, and co-founder of Ushahidi
- **Mexico:** Alejandra Ezeta, Executive Director, Ciudadanos en Medios: Democracia e Información
- **Nigeria:** 'Gbenga Sesan, Executive Director, Paradigm Initiative Nigeria
- **Russia:** Alexey Sidorenko, Managing Editor, RuNet Project at Global Voices Online
- **South Africa:** Jane Duncan, Highway Africa Chair of Media and Information Society, School of Journalism and Media Studies, Rhodes University
- **Southeast Asia** (Advisor): Bridget Welsh, Associate Professor in Political Science, Singapore Management University
- **South Korea:** Yenn Lee, Ph.D. Politics Department, Royal Holloway, University of London
- **Thailand:** Supinya Klangnarong, Vice-Chair, Campaign for Popular Media Reform and Board Member of Thai Netizen Network
- **Turkey:** Yaman Akdeniz, Associate Professor of Law, Istanbul Bilgi University and founder of Cyber-Rights.org
- **United Kingdom**: David Banisar, Senior Legal Counsel for Article 19, London
- **United States**: Lauren Gelman, lecturer at Stanford Law School and founder of the consulting firm BlurryEdge Strategies in San Francisco

The analysts for the reports on Azerbaijan, Bahrain, Belarus, China, Egypt, Ethiopia, Indonesia, Malaysia, Pakistan, Rwanda, Saudi Arabia, Tunisia, Venezuela, Vietnam and Zimbabwe are independent internet researchers who have requested to remain anonymous.

ABOUT FREEDOM HOUSE

Freedom House is an independent private organization supporting the expansion of freedom throughout the world.

Freedom is possible only in democratic political systems in which governments are accountable to their own people, the rule of law prevails, and freedoms of expression, association, and belief are guaranteed. Working directly with courageous men and women around the world to support nonviolent civic initiatives in societies where freedom is threatened, Freedom House functions as a catalyst for change through its unique mix of analysis, advocacy, and action.

- **Analysis:** Freedom House's rigorous research methodology has earned the organization a reputation as the leading source of information on the state of freedom around the globe. Since 1972, Freedom House has published *Freedom in the World*, an annual survey of political rights and civil liberties experienced in every country of the world. The survey is complemented by an annual review of press freedom, an analysis of transitions in the post-communist world, and other publications.
- **Advocacy:** Freedom House seeks to encourage American policymakers, as well as other government and international institutions, to adopt policies that advance human rights and democracy around the world. Freedom House has been instrumental in the founding of the worldwide Community of Democracies, has actively campaigned for a reformed Human Rights Council at the United Nations, and presses the Millennium Challenge Corporation to adhere to high standards of eligibility for recipient countries.
- **Action:** Through exchanges, grants, and technical assistance, Freedom House provides training and support to human rights defenders, civil society organizations, and members of the media in order to strengthen indigenous reform efforts in countries around the globe.

Founded in 1941 by Eleanor Roosevelt, Wendell Willkie, and other Americans concerned with mounting threats to peace and democracy, Freedom House has long been a vigorous proponent of democratic values and a steadfast opponent of dictatorships of the far left and the far right. The organization's diverse Board of Trustees is composed of a bipartisan mix of business and labor leaders, former senior government officials, scholars, and journalists who agree that the promotion of democracy and human rights abroad is vital to America's interests.

1301 Connecticut Avenue, NW, Washington, DC 20036
(202) 296-5101

120 Wall Street, New York, NY 10025
(212) 514-8040