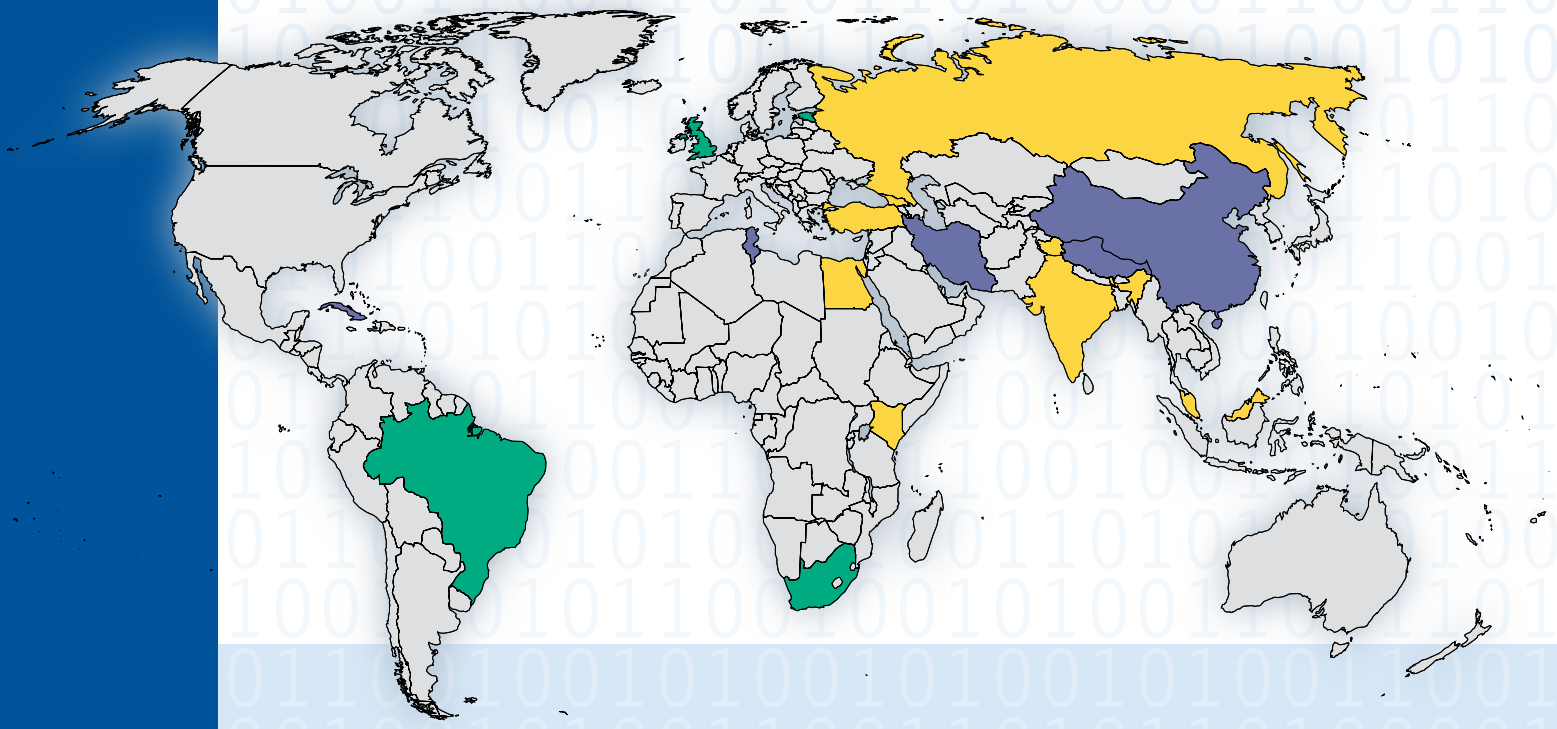
FREEDOM HOUSE

FREEDOM ON THE NET

A GLOBAL ASSESSMENT OF INTERNET AND DIGITAL MEDIA



FREEDOM ON THE NET

A Global Assessment of Internet and Digital Media

April 1, 2009

Table of Contents

Access and Control:

A growing diversity of threats to internet freedom

By Karin Deutsch Karlekar and Sarah G. Cook

As the internet and other new media come to dominate the flow of news and information around the world, governments have responded with measures to control, regulate, and censor the content of blogs, websites, and text messages. Indeed, the recent case of an Iranian blogger who died in police custody is a disturbing reminder that expressions of political dissent or even independent thought circulated through the internet carry as much risk as those circulated via underground journals in an earlier era. And just as authoritarian regimes once devoted massive resources to controlling the print media and the airwaves, so today China employs a small army of functionaries tasked with monitoring and censoring the content of websites and blogs.

The mounting assault on digital freedom is taking place in an environment of explosive growth in the use and, more significantly, the influence of new media forms. An increasing number of organizations and civic initiatives use websites to inform the public about their causes and question government performance. Recent years have also featured a "blogging revolution," as millions of people have begun keeping online journals, commenting and sharing opinions on a vast number of cultural, social, and political issues. This expansion has taken place in developed and developing countries alike, in countries where the press is under duress as well as in vibrant democracies.

Even as new information sources become more prevalent and influential, governments, and in some cases private actors, have begun to push back through the development of techniques designed to control what people read, view, and discuss. Predictably, some of the world's most repressive regimes, like those in China and Iran, have created a pervasive, sophisticated, and multilayered system of censorship that significantly limits the content that citizens can access or post on the internet and transmit via mobile phones, particularly when it comes to topics deemed sensitive by the authorities. Harsh laws, an apparatus of monitoring and surveillance, torture, and imprisonment await those who cross the "red lines" separating acceptable from unacceptable thought. In settings that are somewhat less repressive—such as Egypt, Russia, and Malaysia—the internet has emerged as a haven of relatively free speech in otherwise restrictive media environments. In these societies, however, the space for free comment and open circulation of ideas is slowly closing, as governments devise subtle methods to manipulate online discussion and apply vague and flexible security laws to arrest and intimidate bloggers. As with traditional media, the result of this sophisticated harassment is an insidious form of self-censorship among journalists and commentators. Even in more democratic countries—such as the United Kingdom, Brazil, and Turkey—internet freedom is increasingly undermined by legal harassment, opaque filtering procedures, and expanding surveillance. On the whole, threats to internet freedom are growing and have become more diverse, both in the array of countries that impose restrictions and in the range of methods employed.

This dynamic of increasing digital media use worldwide accompanied by more systematic and sophisticated methods of control is the core finding of this study, a pilot report on internet and new media freedom. On the basis of a newly developed set of 19 indicators, the

study evaluates the level of internet and mobile-phone freedom experienced by average users and activists in a sample of 15 countries across 6 regions: China, India, and Malaysia in Asia; Cuba and Brazil in Latin America; Egypt, Tunisia, and Iran in the Middle East and North Africa; Kenya and South Africa in sub-Saharan Africa; Russia, Estonia, and Georgia in the former Soviet Union; and the United Kingdom and Turkey in Europe. Covering the calendar years 2007 and 2008, the index addresses a range of factors that might affect such freedom, including the state of telecommunications infrastructure, government restrictions on access to technology, the regulatory framework for service providers, censorship and content control, the legal environment, surveillance, and extralegal attacks on users or content producers. The selected indicators capture not only the actions of governments but also the vigor, diversity, and activism of the new media domain in each country, regardless of—or despite—state efforts to restrict usage.

Key findings and trends

Access to and usage of internet and mobile-phone technologies have grown exponentially in recent years. In six of the countries examined, internet penetration doubled between 2006 and 2008, and in three, mobile-phone penetration similarly doubled. This greatly expanded access, however, has been met in most cases with the clear emergence of new and multiple threats to other aspects of internet freedom, particularly restrictions on certain content or heightened prosecution and surveillance of users.

Negative trends:

- **Expanding forms of censorship:** Censorship and control of online content was present in some form in all 15 countries studied, with authorities in 11 targeting political content in at least one instance. Censorship takes a number of forms and can include not only technical filtering, but also manual removal of content as a result of government directives, intimidation, requests from private actors, or judicial decisions. Some regimes even engage in the sophisticated manipulation of online conversations using undercover government-sponsored agents.
- **Privatization of censorship:** There is a growing trend toward "outsourcing" censorship and monitoring to private companies, as opposed to direct intervention by government agencies. In a range of countries with differing levels of democracy, private entities and their employees—including service providers, blog-hosting companies, cybercafes, and mobile-phone operators—are being required by governments or other actors to censor and monitor information and communication technologies (ICTs). This has been the case for local and multinational enterprises alike.
- **Lack of transparency and accountability:** In both democratic and authoritarian settings, there is a serious lack of transparency surrounding censorship decisions and the use of surveillance. In the majority of the countries examined in this study—whether they censor pornography or legitimate political content—there is no public list of blocked websites, little or no possibility of appeal for those who find that content they have posted online is inaccessible to others, and limited independent judicial supervision of the use of information obtained through the monitoring of either the content or the traffic data of internet and mobile-phone communications.

- **Legal threats:** Methods of control and censorship that were developed to restrict content in traditional media—particularly in the legal sphere—are beginning to seep into the new media environment, though they are not yet as common or extensive as in the older context. Multiple countries saw their first blogger sentenced to prison or their first internet-restricting legislation introduced during the coverage period.
- **Technical attacks:** In addition to imprisonment, harassment, torture, and intimidation, internet activists are experiencing forms of "technical violence" that are not present in the traditional media sphere. These hacking or denial-of-service attacks are increasingly being employed by a range of actors, and they are negatively affecting internet freedom in a number of countries.

Positive trends:

- **Poverty not a barrier to new media freedom:** Developing countries, although hindered by infrastructural constraints, can perform well overall in the index if they enact good policies regarding access, content, and the legal framework. From an economic perspective, liberalization of the market for service providers was found to have reduced the cost of access and significantly increased penetration rates in a number of countries.
- **Growing civic activism:** Even in highly repressive countries, citizens are making use of ICTs in inventive ways in order to create and disseminate news and information, add to the diversity of viewpoints and opinions, perform a watchdog role, and mobilize civic groups "offline" in order to address particular political, social, and economic issues.

What the index measures

Freedom on the Net aims to measure each country's level of internet and new media freedom on the basis of two key components – access to the relevant technology and the free flow of information through it without fear of repercussions.

Our assessments reflect not just government actions and policies, but also the impact that actions by non-state actors or foreign governments may have on the user experience within the geographical boundaries of a country. It also reflects the behavior of users themselves in testing boundaries, even in more restrictive environments.

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).

The methodology aims to capture the wide variety of possible factors that could affect levels of internet freedom, as well as providing a way to assess the particular dynamics within each country, both in terms of changing methods of restriction as well as changes over time.

- **Internet freedom greater than press freedom:** Every country examined—with the exception of the United Kingdom—performed better on internet freedom than on media freedom in general, as measured by Freedom House's annual *Freedom of the Press* index. These differences were smaller among the best and the worst performers, and were most pronounced in the middle range of countries.

Wide variation in the environment for internet freedom

A principal aim of the pilot study was to choose a set of countries that demonstrate the varying levels of internet freedom in the world and showcase the range of issues and restrictions that prevail in different media environments.

Free: Countries that scored in the Free range (0–30 points out of a possible 100) include Estonia, clearly the best performer with a total score of 10; the United Kingdom and South Africa, with scores of 20 and 21, respectively; and Brazil, with 26. These countries all have a generally open environment for new media, with few or no government obstacles to access, a low level of content control, and few violations of individual users' rights. Even within this range, however, there are issues of concern. The United Kingdom's score suffered from problems related to libel laws, lack of transparency, and extensive surveillance, while in Brazil judicial decisions that lead to content censorship are a growing threat. In South Africa, many obstacles to access are infrastructural shortcomings rather than deliberate government policies. Estonia stands out as having particularly widespread access and strong protections for user rights and personal data, though it has recently come under pressure from the European Union to change such policies.

"China's apparatus for censoring and controlling content is the most sophisticated and prison sentences imposed the longest."

Partly Free: The middle band of countries ranked in the Partly Free category (31–60) range from relatively strong performers such as Kenya and India to more restrictive environments like Georgia, Malaysia, Turkey, Egypt, and Russia. These countries all have some limits to access (either infrastructural or imposed by the government), some controls or state influence over content and on users' ability to mobilize via digital resources, and varying levels of denial of user rights, including legal interventions, interference with privacy, and physical harassment or attacks. In many of these countries there is a wide gap between internet freedom and the levels of freedom for print and broadcast media. While digital media do face efforts at state control in these societies, the internet and other new technologies serve as relatively open outlets in what are otherwise difficult environments for freedom of expression.

Not Free: In the Not Free category (61–100) are China, Iran, and Tunisia, which all have significant government-imposed restrictions on access to certain technologies, extensive technological filtering and other forms of content control, and systematic violations of user rights, including prosecutions, extralegal attacks, and invasion of privacy. Of the three, China's apparatus for censoring and controlling content is the most sophisticated and prison sentences imposed the longest, while in Tunisia and Iran, there are greater infrastructural limitations on usage. Although the level of internet freedom is higher than that of general media freedom and provides a key open space in restrictive media environments, these governments all take a range of measures to control the new media and are especially determined to prevent them from facilitating the mobilization of political opposition.

Worst of the Worst: Rounding out the pilot study is Cuba, which received a score of 90. Cuba stands out due to its near-total restrictions on access to internet and mobile-phone technology, whereas other countries promote internet use but then seek to control content or engage in harsh retaliatory measures against individual bloggers and online activists. Censorship of content, severe limitations on residents' ability to use digital technologies as news sources or for mobilization, stringent legal penalties, and disregard for privacy rights all

ensure the Cuban regime's almost absolute control over the internet, despite small openings in the last few years.

Typologies by category

In addition to the breakdown of the countries studied into Free, Partly Free, and Not Free according to their total score, additional typologies emerged based on scoring in each of the three topical categories: Obstacles to Access, Limitations on Content, and Violations of User Rights.

Similar performance across all three aspects of internet freedom: The group of countries that exhibited this dynamic included Estonia, which scored well across the board, as well as Georgia, which received moderate scores in all three categories, thanks in part to restrictions on internet freedom stemming from a much less favorable traditional media environment. The fact that Iran, China, and Tunisia also fit into this group reflected their governments' multilayered and comprehensive approach to controlling internet and mobile-phone usage.

Weak performance on access to technology: Not surprisingly, the countries fitting this pattern included developing countries with relatively low gross national income per capita—India, Kenya, and South Africa. For the two African countries, however, their weak performance in the Obstacles to Access category was matched by relatively strong respect for user rights, with only Estonia scoring better in that category. Also in this group was Cuba, where despite heavy limitations on content and extensive violations of user rights, the most significant restriction on internet freedom is the sheer lack of access to the technology, largely due to government actions. Cuba received the worst possible score in the Obstacles to Access category.

Categories

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

Obstacles to Access: assesses governmental efforts to block specific applications or technologies; infrastructural and economic barriers to access; 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.

Particularly high degree of violations of user rights: Six countries reflected this dynamic, making it the most common typology. On the one hand, the group included Russia, Egypt, and Malaysia, where government-encouraged improvements in access to ICTs and relatively little censorship are offset by harsh legal environments, state monitoring, and a rise in criminal prosecutions. On the other hand, the description also fit the more democratic United Kingdom, Brazil, and Turkey. While criminal prosecutions for legitimate online activities rarely occur in these societies, they do suffer from the threat of prosecution or restrictions associated with civil lawsuits for libel and defamation. In addition, fairly extensive requirements are placed on

service providers to retain user data or filter certain content. The United Kingdom's score in this category was striking, given that it scored a perfect 0 on Obstacles to Access.

Threats to internet freedom and methods of control

As mentioned above, a key finding of the study was the wide range of threats to internet freedom. The methods of control vary and are used with increasing frequency. They include:

Restricting access to technologies or applications: The index divides obstacles to accessing relevant ICTs into two types: deliberate government attempts to restrict access to particular technologies or applications, and other limitations that may occur as a result of infrastructural or economic constraints. For the first category, practices covered the entire spectrum: in four countries—Estonia, Russia, South Africa, and the United Kingdom—there were no official attempts to restrict technologies, while in several others—such as China, Malaysia, and Tunisia—the restrictions were limited in scope, either sporadically interfering with access due to specific events or selectively targeting particular activists. On this indicator, Iran stands out for its decision to limit broadband access for the majority of internet users, while Cuba largely cuts off its population from internet access altogether and only recently relaxed restrictions on mobile-phone ownership.

Regarding specific applications, the study found that seven countries had blocked so-called Web 2.0 applications—advanced services such as the social-networking site Facebook, the video-sharing site YouTube, and the blog-hosting site Blogspot—either temporarily or permanently during the 2007–08 coverage period. Such applications are among the most popular features of the internet and exemplify the interactive potential of the medium. They enable production of content and circulation of information by any user and are often at the center of exposures of government malfeasance or antigovernment mobilizations. Because information can be spread quickly using these applications, some governments have moved to block access to entire sites rather than selectively removing content after it has been posted. Turkish and Brazilian courts and regulatory bodies have resorted to this tactic; Turkey has blocked YouTube since May 2008. While the international versions of such applications are generally blocked in China, they have been replaced by domestic alternatives, allowing users to share videos or maintain blogs. However, as Chinese companies are more susceptible to government pressure and censorship directives than their foreign counterparts, such a replacement dynamic essentially serves as a means of exercising greater control over content.

> ***"Seven of the 15 countries studied blocked so-called Web 2.0 applications—such as Facebook, YouTube, Blogspot—at some point during 2007 and 2008."***

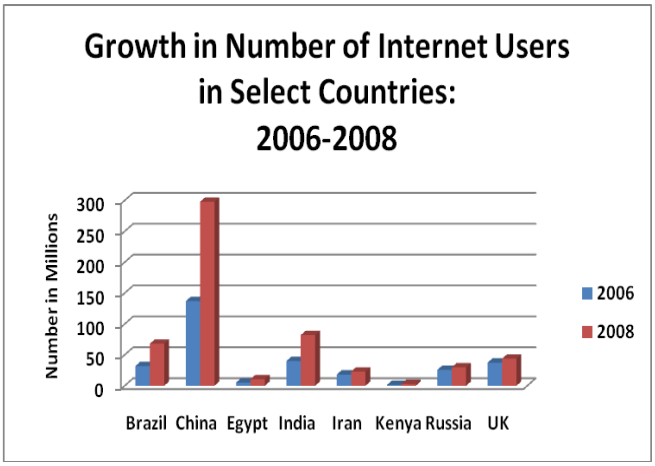
Economic obstacles to access: The study found, understandably, that infrastructural and economic constraints were the main or among the main obstacles in countries with lower gross national income per capita and other socio-economic indicators. For example, Georgia, India, Kenya, and South Africa, which all performed relatively well overall, scored poorly on these questions. Internet penetration rates in these countries tended to be low, costs for access were high compared with income, there was a significant rural-urban divide with regard to level of access, and there was a relatively low level of broadband penetration. At the same time, mobile-phone penetration was often significantly higher than internet penetration in these countries, reaching between 30 and 90 percent of the population with fairly widespread geographic coverage. In some countries, this has contributed to an increase in

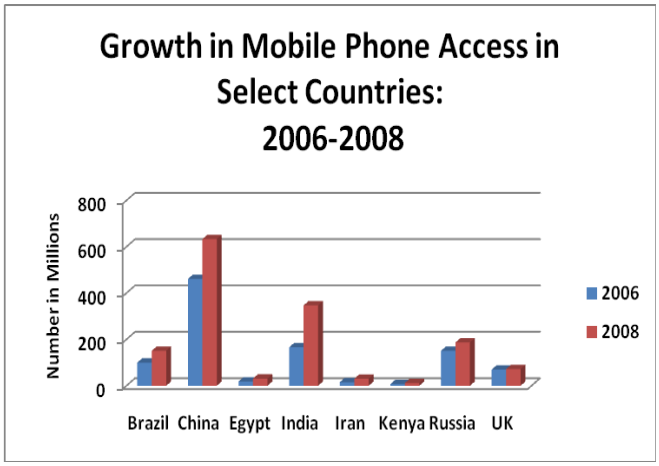
the number of individuals accessing the web via their mobile phones. Indeed, South Africa was in the unique position of having more people access the internet via the "mobile web" than from computers.

The study also found that developing countries that made decisions to promote broader or cheaper access, such as Egypt, Brazil, Malaysia, Turkey, and China, scored relatively well on these questions. Thus even in developing societies, government action can reduce the impact of poverty as a barrier to internet use, although the rural-urban divide and low computer literacy remain key challenges. Cuba, by contrast, remains a society in which inadequate infrastructure and prohibitively high government-imposed pricing stand as insuperable obstacles to expanded internet access.

Filtering and censorship: One of the primary ways to restrict internet freedom is to prevent users from accessing content that is deemed undesirable by the authorities. This can be accomplished through the technical filtering of either specific content or broad swaths of information at the ISP level, targeting keywords, entire domain names, or particular web addresses. Pioneering technical tests conducted by the OpenNet Initiative have shown a dramatic increase in filtering over the past several years, with a growing number of countries engaging in some form of the practice. However, this study found that states employed a range of additional methods to limit access to content and control the circulation of information, including human censors who monitor and manually remove blog postings; outsourcing of search-engine filtering and chat-room censorship to private companies; judicial orders or instructions from a regulator to remove certain content; and either written or informal requests from authorities to ISPs, websites, or blog hosts to take down proscribed materials.

Of the 15 countries in the study, only three—China, Iran, and Tunisia—filtered political content using systematic technical means. It was found that comprehensive filtering was possible in large part because all three countries have centralized their internet infrastructure so that all traffic must pass through a limited number of gateways or service providers, particularly before connecting to the global internet. In these countries, there is pervasive filtering of permanently taboo topics, including those related to human rights violations, prominent political figures, oppressed minorities, and official corruption. Proscribed content is identified through lists of forbidden keywords or website addresses, and the lists are regularly updated by state agencies based on real-world developments. Among the three countries, however, China was the only one found to have engaged in similarly systematic filtering of mobile-phone text messages.





A number of other countries that eschewed extensive filtering still imposed relatively serious blocks on certain websites or types of political content. This included opposition news sources in Malaysia; content related to ethnic minorities or deemed insulting to the national identity in Turkey; and briefly in Georgia, all sites whose domain names ended with Russia's ".ru" country code. Russian authorities relied to a larger extent on behind-the-scenes pressure or phone calls requesting the removal of certain content. This method was also employed by Chinese authorities, who send out regular guidance on acceptable content as well as where and how it should be posted or deleted. Among the better performers, filtering or blocking tended to target small amounts of well-defined content, such as child pornography, although there were instances in which blocks were employed to censor sensitive political or social content, or caused larger obstructions than were intended. Several countries, including Egypt, Kenya, South Africa, and Estonia, were notable for blocking almost no content, including material that might be deemed politically sensitive.

Content manipulation: Even with sophisticated filtering technology, it is effectively impossible to create an airtight "firewall" against all content deemed undesirable by the government. With the exception of Cuba, all the countries in the study have some degree of content diversity, and a variety of opinions reach at least certain sections of the population, particularly those that are versed in circumvention techniques. Thus authoritarian regimes have increasingly resorted to guiding or influencing online discussion through the clandestine use of paid progovernment commentators or the financing of entire websites and blogs. The Chinese government employs an estimated 250,000 "50 Cent Party" commentators, Russia has seen a proliferation of Kremlin-affiliated "content providers," and Tunisia uses a smaller team of undercover agents, all essentially aiming to subvert any online conversations that might erode support for the regime. A related dynamic is the spillover effect of tightly controlled traditional media outlets that launch online versions, remain key sources of information for many ordinary users, and are thus able to shape online opinions.

"Outsourcing" of censorship and surveillance to private companies: Partly due to the nature of internet and mobile-phone technologies, extensive censorship and monitoring of content or usage patterns are not possible without the cooperation of private companies. Consequently, every country assessed in this study was found to engage in some level of "outsourcing" to nongovernmental access providers, be they ISPs, cybercafes, or mobile-phone operators. Among good and mid-range performers—such as Estonia, Kenya, South Africa, Georgia, Malaysia, the United Kingdom, and India—this took the form of legislation requiring retention of user data, interception powers for law enforcement agencies (often with some judicial oversight), or filtering of content, although the targeted material did not involve political communication in these relatively free settings. In more authoritarian environments—such as Egypt, China, Tunisia, Cuba, and Iran—the outsourcing involved extensive surveillance and user registration, especially in cybercafes; legal requirements for the filtering of political content; and sanctions such as the loss of business licenses for private entities that failed to comply with regulations. In China, Iran, and Tunisia, private entities often had significant numbers of staff members assigned to implement these tasks, which imposed an additional cost on their businesses. In these three countries in particular, international technology companies have also complied with the local, illiberal, and antidemocratic regulations. They have aided censorship and surveillance practices, provided equipment that is crucial to carrying out such tasks, and at times turned over the personal data of users, leading to their arrest.

Legal repercussions: Most countries do not have internet-specific criminal legislation but rely on general press laws or statutes against insult, blasphemy, leaking state secrets, and other prohibitions to restrict or punish users for online activities. Overall, in 6 of the 15 countries under assessment, a blogger or online journalist was sentenced to prison during the coverage period. Cuba is one of the few countries with internet-specific laws, but tends to prosecute online journalists under generic charges such as presenting a "precriminal social danger." The level of prosecutions is highest in China, which uses laws against "inciting subversion," "leaking state secrets," and "using a heretical organization to undermine the law," and has issued more than 80 decrees that specifically address internet content and related issues. Prison sentences for online violations in China tend to be longer than elsewhere, with a typical minimum of three years and maximums as high as ten, while in other countries most sentences range from six months to four years. Numerous prosecutions have also occurred in Tunisia, Iran, Egypt, and Malaysia, where laws against insulting the head of state or Islam are most frequently invoked, while Russia relies on vague laws against extremism. Even better performing countries like India produce occasional cases against bloggers. By contrast, legal repercussions for online activity seem to be virtually nonexistent in South Africa, Kenya, and Georgia. Although Turkey is notorious for its high rate of prosecutions against journalists and writers in general, it would appear that this has not yet affected online content producers to the same extent. In the United Kingdom, the phenomenon of "libel tourism" poses a new threat to journalists and scholars alike. Wealthy individuals from the Middle East and the former Soviet Union have exploited expansive interpretations of libel laws and jurisdictional questions by British courts to silence or intimidate journalists through civil lawsuits, leading to increased self-censorship among both traditional and online commentators, particularly on issues related to the financing of terrorism.

"In 6 of the 15 countries assessed, a blogger or online journalist was sentenced to prison."

Extralegal harassment and threats: The extralegal punishment of individuals for their online activities has emerged as a major and growing issue of concern. The Committee to Protect Journalists noted at the end of 2008 that there were more online journalists than traditional journalists behind bars for the first time that year, either as a result of legal prosecution or extralegal detention. Such forms of repression are virtually unknown in the better-performing countries, although there have been exceptions. At least one blogger or journalist was detained during the coverage period in 8 of the 15 countries under study, in some cases for a short period of time. However, the intimidation of individuals has reached significant proportions in 6 of the 15 countries. In these cases, multiple individuals have been subjected to arbitrary arrest, 24-hour surveillance, harassment, prosecution, or various forms of mental and physical mistreatment, including torture. Levels of abuse are particularly severe in China, Egypt, Iran, and Tunisia. Egypt stands out as a country with a relatively open internet environment that has chosen to use these methods to make an example of a few prominent activists and bloggers. Although the number of individuals targeted in these countries is small relative to the entire online community, their experiences have a chilling effect on their peers.

Harassment can also take the form of "technical violence," in which specific websites or servers are attacked by hackers employing dedicated denial of service (DDoS) attacks, which can paralyze or shut down entire websites. Such incidents occurred in six countries; in Georgia and Estonia, massive attacks targeted government websites and information networks during periods of diplomatic or military friction with Russia. The assaults were apparently carried out by

individuals residing in Russia and possibly associated with the Russian authorities.

Positive openings

Despite the growing range of threats and methods of control, there have been several positive trends in recent years. As access to the relevant technologies has expanded, so too has the circulation of news and information and user mobilization on a host of political and social issues. Even in Cuba, with its tight controls on access, some citizens have attempted to push the boundaries through blogging and the offline sharing of downloaded internet content through USB devices and other means.

In other restricted media environments, the diversity of online content is significantly higher than in the print and broadcast media, and citizens have to some extent been able to use the internet and mobile phones to spread information and organize around certain issues. This is more easily done on topics deemed less threatening to the government, such as environmental activism in Iran or relief efforts after the Sichuan earthquake in China. But it is also present to a degree on more politically sensitive subjects, such as women's rights in Iran or calls for an end to one-party rule in China. Online activism is especially striking in middle-range performers such as Malaysia and Egypt, where citizens have used blogs and social-networking sites to organize protests and create pressure groups pertaining to government policies or local elections. In Kenya, an online citizen journalism initiative called Ushahidi was launched during a burst of postelection ethnic violence. It catalogued incidents using messages sent by ordinary citizens with their mobile phones, and posted them onto a map to track the unfolding events.

Some governments have taken positive steps to strengthen online freedom. In Brazil and Egypt, the authorities have introduced programs to support the opening of low-cost internet access points in rural and economically disadvantaged areas. In Estonia, the government has opened over 1,200 free wireless internet-access zones, with at least 800 more planned for the coming year. In Turkey, a parliamentary inquiry has been launched into surveillance practices by law enforcement agencies following a series of scandals. There have also been several court decisions upholding freedom of speech online. In South Africa, a judge ruled that ISPs should not be held liable for comments posted by users, while in Egypt a court rejected a request to block several dozen websites, including those of prominent human rights groups.

Future trends

- **Growth of the "mobile web":** A noticeable trend, particularly among developing countries, is the growing availability and affordability of internet access via mobile phones, whose penetration rate is currently higher in most countries than that of the internet. This process holds the potential for both positive and negative effects on internet freedom. On the one hand, the number of individuals able to make use of the internet will grow exponentially. On the other hand, the methods already used by governments to restrict the content viewed or transmitted via computers may spread to the "mobile web." Indeed, some of the findings of this report indicate that such a dynamic is beginning to emerge, as China, Tunisia, and Iran channel mobile internet traffic through the same gateways as traditional internet traffic, subjecting it to similar levels of monitoring and technical filtering.

- **Expanded adoption of sophisticated censorship and filtering methods:** As internet and mobile-phone access continues to grow, more and more governments may respond by implementing sophisticated censorship and filtering mechanisms. This possibility poses a threat particularly in

middle-performing countries where the internet environment has thus far been significantly more open than the traditional media sphere. Countries to watch in this regard are Egypt, Kenya, Georgia, Malaysia, and Russia, as their scores on this index are notably better than on Freedom House's press freedom index.

- **Increase in legal repercussions and violations of user rights:** As the findings of this study indicate, the first line of attack in many countries—whether democratic or authoritarian—is legal sanctions and violations of user rights. Without persistent public pressure and vigilant oversight by the international community, this trend could continue, with more countries passing restrictive, internet-specific criminal legislation; more powerful societal actors using defamation suits to silence critics; and more bloggers being sentenced to long prison terms, tortured, or killed. Indeed, since the end of this study's coverage period, Kenya's president has ratified a controversial cybercrimes bill, a prominent Chinese blogger has been stabbed in a public place, and an Iranian blogger has died in prison.

Despite such threats, the flexibility and spread of digital media technology carry with them significant promise for improving the flow of information, enhancing civic participation and activism, and ultimately, bringing greater freedom to all corners of the globe. Nonetheless, as this study's findings indicate, such potential must not be taken for granted. Foresight and creativity are needed, particularly on the part of democratic countries, to develop policies and procedures that are applicable to new technologies but consistent with international standards for human rights and democratic governance. In a fast-changing digital world, vigilance is required if we are to ensure continued freedom on the net.

***

Karin Deutsch Karlekar, a senior researcher at Freedom House, served as managing editor of the pilot Freedom on the Net: A Global Assessment of Internet and Digital Media. *She holds a PhD from Cambridge University. Sarah Cook, an Asia researcher at Freedom House, served as assistant editor of the study. She holds masters degrees in politics and international law from the University of London's School of Oriental and African Studies.*

Overall guidance for the project was provided by Robert Guerra, project director of Freedom House's Global Internet Freedom Initiative; Christopher Walker, director of studies; Daniel Calingaert, deputy director of programs; and Arch Puddington, director of research. Extensive research, editorial, proofreading, and administrative assistance was provided by Denelle Burns, as well as by Tyler Roylance, Katrina Neubauer, Joanna Perry, Eliza Bonner, Caroline Neilsen, and interns Joshua Siegel, Eliza Young, and Aidan Gould. We would like to thank our consultant writers and advisers and other members of the survey team for their contributions. We are also very appreciative of numerous individuals who provided guidance and feedback on the methodology developed for this pilot study.

This project was made possible by contributions from the U.S. Department of State Bureau of Democracy, Human Rights and Labor, the United States Agency for International Development (USAID), and the Dutch Foreign Ministry. Freedom House is actively seeking additional funding to expand and continue this pilot study.

Freedom on the Net Methodology

This 2009 pilot *Freedom on the Net* provides analytical reports and numerical ratings for 15 strategic countries. The countries were chosen in order to provide a representative sample with regard to geographical and regional diversity and economic development, as well as varying levels of internet and digital media freedom. The ratings and reports included in this pilot primarily cover events that took place between January 1, 2007, and December 31, 2008.

What we measure

The *Freedom on the Net* index aims to measure each country's level of internet and digital media freedom on the basis of two key components—access to the relevant technology and the free flow of information through it without fear of repercussions. Given increasing technological convergence, the index measures not only internet freedom, but also access and openness of other digital means of news media transmission, particularly mobile phones and text messaging services.

Freedom House does not maintain a culture-bound view of freedom. The index 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.

In measuring digital media freedom, the index is particularly concerned with 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 the 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 insurgents and other armed groups, 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 19 methodology questions, divided into three categories, which are intended to highlight the vast range of issues that can impact digital media freedom. 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 category. The degree to which conditions in each country enable the free flow of news and information via the internet and other information and communication technologies (ICTs) determines their overall classification as "Free," "Partly Free," or "Not Free." Countries scoring from 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 and ICT freedom through a set of 19 questions and 90 subquestions, organized into three baskets:

- ***Obstacles to Access***—including governmental efforts to block specific applications or technologies; infrastructural and economic barriers to access; and 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 other privacy violations; and repercussions for online activity, such as prosecution, imprisonment, physical attacks, and other forms of harassment

Index Checklist 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 is Free, 31–60 is Partly Free, and 61–100 is Not Free.
- Under each question, a lower number of points is allotted for a more free situation, while a hi number of points is allotted for a less free environment.
- Unless otherwise indicated, the subquestions listed are meant to provide guidance as to what

A. Obstacles to Access (0–25 points)

1. **Does the government block access to digital media or 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?*
   - *Does the government centralize telecommunications infrastructure to 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 (e.g., Facebook)?*
   - *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.)?*
   - *Is there blocking of certain tools that enable circumvention of online filters and censors?*

2. **Do infrastructural limitations restrict access to internet and other ICTs? (0–6 points)**
   - *Does poor infrastructure (electricity, telecommunications, etc.) limit citizens' ability to receive internet in their homes and businesses?*
   - *Is there widespread public access to the internet through internet cafés, libraries, or other venues?*
   - *Is there a high degree of internet and mobile-phone penetration?*
   - *Is there a significant difference between internet penetration and access in rural versus urban areas?*
   - *Are broadband services available in addition to dial-up?*

3. **Is access to the internet and other ICTs prohibitively expensive or beyond reach of certain segments of the population? (0–3 points)**
   - *In command economies, does the state set the price of internet access prohibitively high?*
   - *Do financial constraints, such as high costs of telephone/internet 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?*
   - *To what extent are online software, news, and other information available in the main local languages spoken in the country?*

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 monopoly in place or do users have a choice among access providers, including some that are 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 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 appointment process transparent and representative of different stakeholders' interests?*
   - *Are decisions taken by the regulatory body 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?*

B. Limits on Content (0–35 points)

1. **To what extent does the state censor internet and other ICT content, particularly on political and social issues? (0–8 points)**
   - *Is there significant blocking or filtering of internet sites, web pages, blogs, data centers, or text-messaging content, particularly those related to political and social topics?*
   - *Are other procedures—judicial or extralegal—used to order the removal of content from the internet, either prior to or after its publication?*
   - *Are certain contentious issues, such as official corruption, the role of the armed forces or the political opposition, human rights, religion, or foreign news sites systematically targeted for online censorship?*
   - *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—to prevent them from reaching the outside world, for example by intercepting e-mail, text messages, etc.?*

2. **To what extent is censorship of 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 procedures in place to ensure that decisions to censor content are legitimate and proportional to their stated aim?*
    - *Are state authorities transparent about what content is blocked or filtered (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?*

3. **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 both state-run online media and privately run websites?*
    - *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 censorship or harm to the author?*

4. **To what extent is the content of online sources of information determined or subtly manipulated by the government or a particular partisan interest? (0–6 points)**
    - *To what degree do the government or nonstate actors subject online news outlets to editorial direction or pressure?*
    - *Do authorities issue official guidelines or directives on coverage to online media outlets, blogs, etc.?*
    - *Are the funding, ownership, and management of websites transparent?*
    - *Do government officials or other actors bribe or otherwise put economic pressure on online journalists, bloggers, website owners, or service providers in order to influence the online content they produce or host?*
    - *Does the government employ, or require access providers to employ, individuals to post progovernment remarks in online bulletin boards and chat rooms?*

5. **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, including those of vulnerable or marginalized groups in society?*
    - *To what extent do users employ proxy servers and other methods to circumvent state censorship efforts?*

6. **To what extent are individuals able to use the internet and other ICTs 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 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 are online communication or social-networking sites used as a means to organize politically, including for "real-life" activities?*
- *Are mobile phones and other ICTs used as a medium of news dissemination and political organization, including on otherwise banned topics?*

7. 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)

- *Is there a high degree of ownership concentration within the online services and advertising industry?*
- *Are connections with government officials necessary for online media outlets to be economically viable?*
- *Are users required to pay varying fees for different degrees of access and publication rights (i.e., are there limitations on "net neutrality")?*
- *Do users have access to free or low-cost blogging services, web hosts, etc. that allow them to make use of the internet to express their own views?*
- *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?*

C. Violations of User Rights (0–40 points)

1. To what extent do the constitution and 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 for their online activities?*

2. Are there laws that assign 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 narrowly defined, closely 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., do the laws encourage "libel tourism" and similar practices)?*

3. **Are individuals prosecuted or punished by other legal means for posting or accessing information on the internet or disseminating information 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 hinder fair proceedings in ICT-related cases?*
   - *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 must 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?*
   - *Can the government obtain information about users without legal process?*

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 text messages?*
   - *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 without government interference?*
   - *Is content intercepted during internet surveillance admissible in court?*

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

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

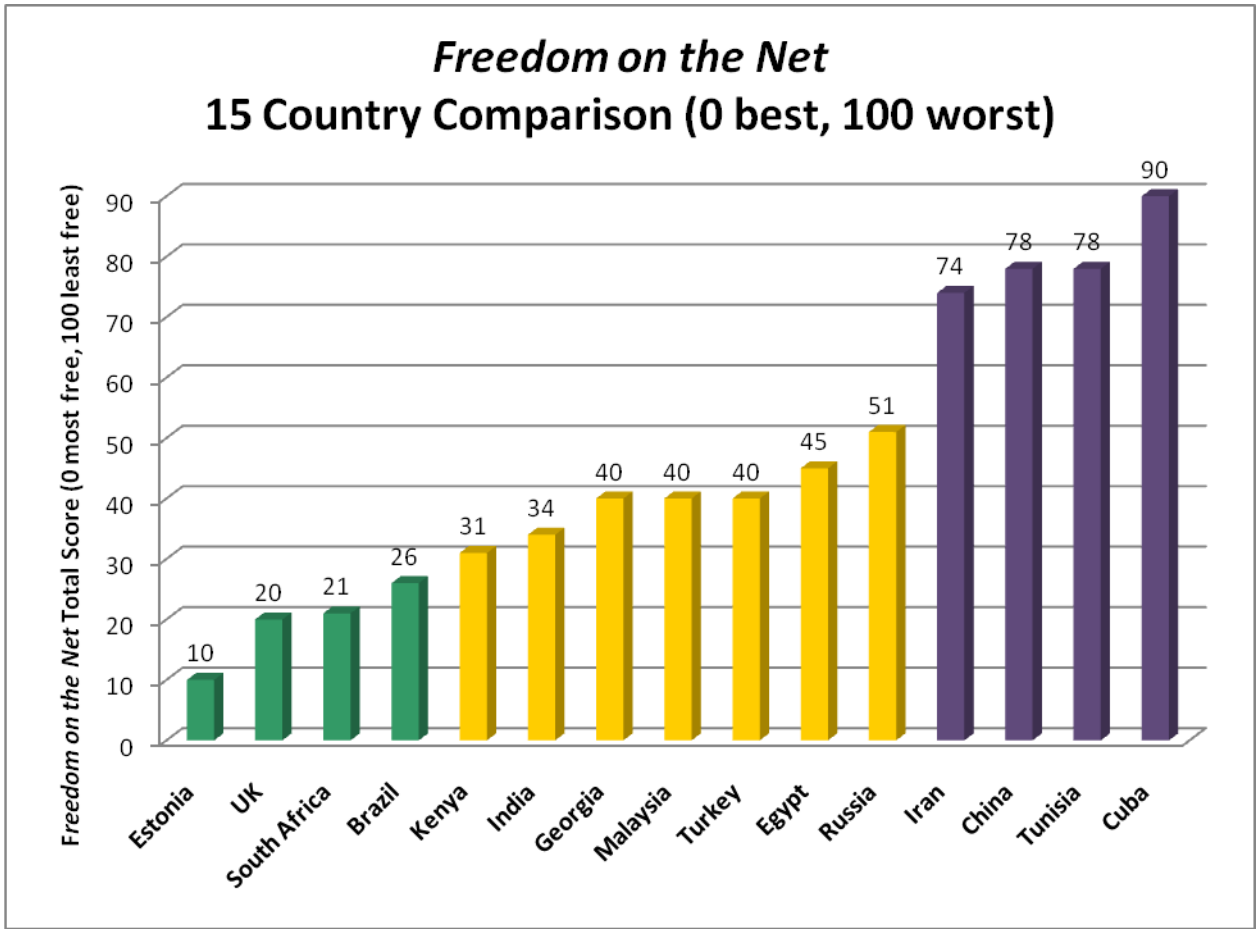
   1a. Internet-service providers (ISPs) and other backbone internet providers (0–2 points)
   1b. Cybercafes and other businesses that allow public internet access (0–2 points)
   1c. Mobile-phone companies (0–2 points)

- *Are access providers legally responsible for the content transmitted via the technology they supply, and are they prosecuted for opinions expressed by third parties via such technology?*
- *Are access providers legally required to filter the content accessed or transmitted by their users?*
- *Are access providers required to monitor their users and supply information about their digital activities to the government (through either technical interception or 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?*

7. Are bloggers, other ICT users, websites, or service providers subject to extralegal intimidation, physical violence, or technical attacks by state authorities or any other actor? (0–8 points)

- *Are individuals subject to murder, injury, harassment, threats, abduction, expulsion, arbitrary detention, 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?*
- *Are websites or blogs subject to targeted "technical violence," such as service attacks, hacking, etc., as a result of their content?*
- *Have cybercafes or property of online commentators been targets of physical attacks or the confiscation or destruction of property?*

Charts and Graphs of Key Findings



* 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.

Freedom on the Net: Main Score Table

Country	*Freedom on the Net* Status	*Freedom on the Net* Total Score *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
UK	**Free**	**20**	0	6	14
South Africa	**Free**	**21**	6	7	8
Brazil	**Free**	**26**	5	8	13
Kenya	**Partly Free**	**31**	10	12	9
India	**Partly Free**	**34**	11	8	15
Georgia	**Partly Free**	**40**	13	15	12
Malaysia	**Partly Free**	**40**	8	12	20
Turkey	**Partly Free**	**40**	11	13	16
Egypt	**Partly Free**	**45**	8	11	26
Russia	**Partly Free**	**51**	11	17	23
Iran	**Not Free**	**74**	19	24	31
China	**Not Free**	**78**	18	27	33
Tunisia	**Not Free**	**78**	20	27	31
Cuba	**Not Free**	**90**	25	32	33

Subtotal Category Explanations:
A Subtotal—Obstacles to Access (0-25 points): Infrastructure, blocking of technology, regulatory framework
B Subtotal—Limits on Content (0-35 points): Censorship, other manipulation of content, blogosphere diversity and mobilization
C Subtotal—Violations of User Rights (0-40 points): Legal environment, surveillance, extra-legal attacks

Freedom on the Net:

Comparison of Obstacles to Access Results

Country	*Freedom on the Net* Status	A Subtotal: Obstacles to Access *0-25 Points*
UK	**Free**	**0**
Estonia	**Free**	**2**
Brazil	**Free**	**5**
South Africa	**Free**	**6**
Malaysia	**Partly Free**	**8**
Egypt	**Partly Free**	**8**
Kenya	**Partly Free**	**10**
India	**Partly Free**	**11**
Turkey	**Partly Free**	**11**
Russia	**Partly Free**	**11**
Georgia	**Partly Free**	**13**
China	**Not Free**	**18**
Iran	**Not Free**	**19**
Tunisia	**Not Free**	**20**
Cuba	**Not Free**	**25**

A Subtotal—Obstacles to Access (0-25 points):
Infrastructure, blocking of technology, regulatory framework

Freedom on the Net:

Comparison of Limits on Content Results

Country	*Freedom on the Net* Status	B Subtotal: Limits on Content *0-35 Points*
Estonia	Free	2
UK	Free	6
South Africa	Free	7
Brazil	Free	8
India	Partly Free	8
Egypt	Partly Free	11
Kenya	Partly Free	12
Malaysia	Partly Free	12
Turkey	Partly Free	13
Georgia	Partly Free	15
Russia	Partly Free	17
Iran	Not Free	24
China	Not Free	27
Tunisia	Not Free	27
Cuba	Not Free	32

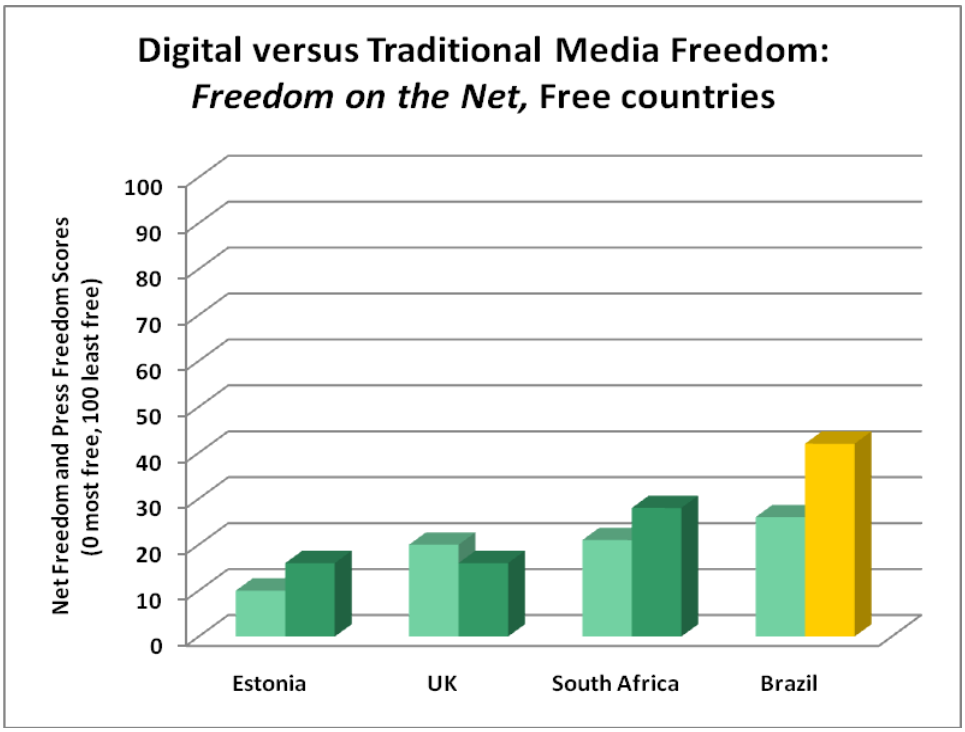
B Subtotal—Limits on Content (0-35 points):
Censorship, other manipulation of content, blogosphere diversity and mobilization

Freedom on the Net:

Comparison of Violations of User Rights Results

Country	*Freedom on the Net* Status	C Subtotal: Violations of User Rights *0-40 Points*
Estonia	Free	6
South Africa	Free	8
Kenya	Partly Free	9
Georgia	Partly Free	12
Brazil	Free	13
UK	Free	14
India	Partly Free	15
Turkey	Partly Free	16
Malaysia	Partly Free	20
Russia	Partly Free	23
Egypt	Partly Free	26
Iran	Not Free	31
Tunisia	Not Free	31
China	Not Free	33
Cuba	Not Free	33

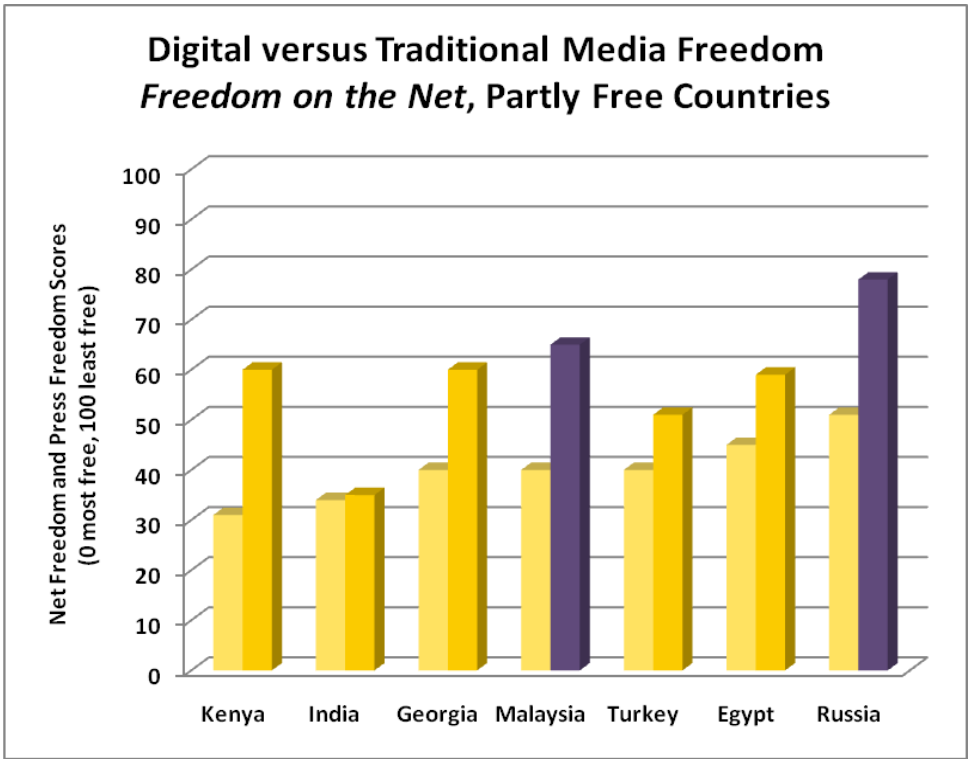
C Subtotal—Violations of User Rights (0-40 points): Legal environment, surveillance, extra-legal attacks



* The left-hand bar represents a country's *Freedom on the Net* total score; the right-hand bar reflects the country's total score on Freedom House's *Freedom of the Press* 2008 index, which primarily assesses television, radio, print media.

* A green-colored bar represents a status of **"Free,"** while a yellow one, the status of **"Partly Free."**

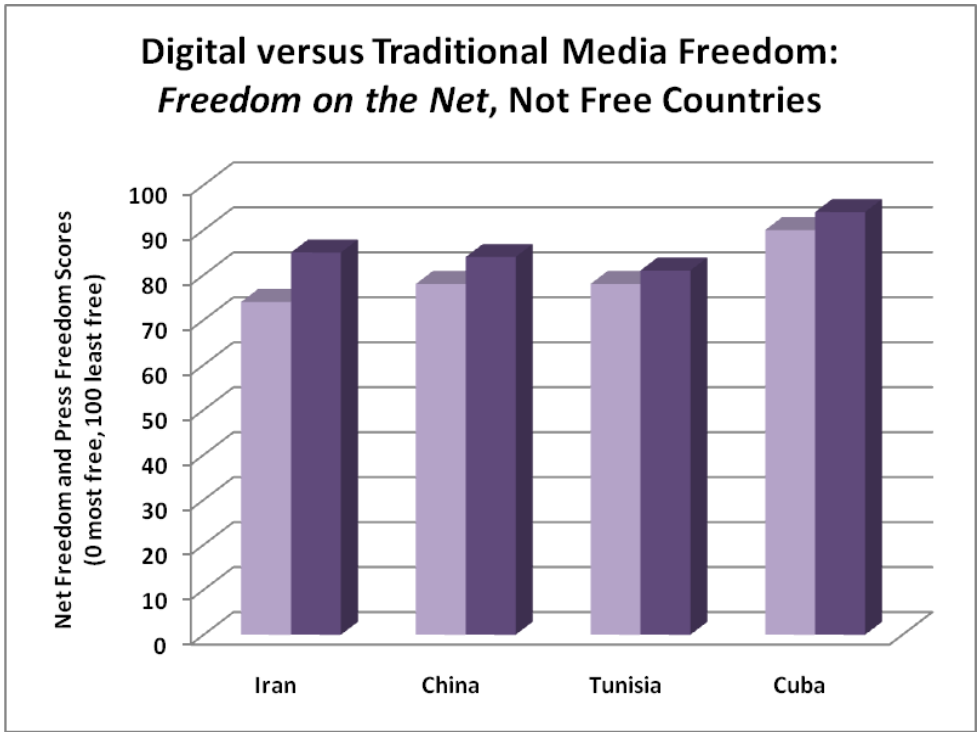
Country	***Freedom on the Net* Total Score** *0-100 Points*	***Freedom on the Net* Status**	***Freedom of the Press* Total Score** *0-100 Points*	***Freedom of the Press* Status**
Estonia	**10**	**Free**	**16**	**Free**
UK	**20**	**Free**	**16**	**Free**
South Africa	**21**	**Free**	**28**	**Free**
Brazil	**26**	**Free**	**42**	**Partly Free**



* The left-hand bar represents a country's *Freedom on the Net* total score; the right-hand bar reflects the country's total score on Freedom House's *Freedom of the Press* 2008 index, which primarily assesses television, radio, print media.

* A yellow-colored bar represents a status of "**Partly Free,**" while a purple one, the status of **"Not Free."**

Country	*Freedom on the Net* Total Score *0-100 Points*	*Freedom on the Net* Status	*Freedom of the Press* Total Score *0-100 Points*	*Freedom of the Press* Status
Kenya	**31**	**Partly Free**	**60**	**Partly Free**
India	**34**	**Partly Free**	**35**	**Partly Free**
Georgia	**40**	**Partly Free**	**60**	**Partly Free**
Malaysia	**40**	**Partly Free**	**65**	**Not Free**
Turkey	**40**	**Partly Free**	**51**	**Partly Free**
Egypt	**45**	**Partly Free**	**59**	**Partly Free**
Russia	**51**	**Partly Free**	**78**	**Not Free**



* The left-hand bar represents a country's *Freedom on the Net* total score; the right-hand bar reflects the country's total score on Freedom House's *Freedom of the Press* 2008 index, which primarily assesses television, radio, print media.

* A purple-colored bar represents a status of **"Not Free."**

Country	*Freedom on the Net* Total Score *0-100 Points*	*Freedom on the Net* Status	*Freedom of the Press* Total Score *0-100 Points*	*Freedom of the Press* Status
Iran	**74**	**Not Free**	**85**	**Not Free**
China	**78**	**Not Free**	**84**	**Not Free**
Tunisia	**78**	**Not Free**	**91**	**Not Free**
Cuba	**90**	**Not Free**	**94**	**Not Free**

Country Reports

Brazil

Status: Free

Obstacles to Access: **5** (0–25)
Limits on Content: **8** (0–35)
Violations of User Rights: **13** (0–40)
Total Score: **26** (0–100)

Population: 194 million
Internet Users/Penetration 2006: 32 million / 17 percent
Internet Users/Penetration 2008: 68 million / 35 percent
Mobile Phone Users/Penetration 2006: 100 million
Mobile Phone Users/Penetration 2008: 151 million
Freedom of the Press (2008) Score/Status: 42 / Partly Free
Digital Opportunity Index (2006) Ranking: 65 out of 181
GNI Per Capita (PPP): $9,400
Web 2.0 Applications Blocked: Yes
Political Content Systematically Filtered: No
Bloggers/Online Journalists Arrested: No

Introduction

For a country with large social disparities, Brazil has made significant gains in expanding internet access and mobile-phone usage in recent years. It is home to the largest population of internet users in Latin America and the seventh largest in the world.[1] The country first connected to the internet in 1990,[2] and connectivity is now available in most areas through a variety of technologies, though some infrastructural limitations remain. While internet use has been mostly unrestricted in the past, several legal actions threatened free online expression in 2007 and 2008, including court decisions leading to censorship of reporting that was critical of politicians, a ban on political campaigning on the Orkut social-networking platform, and proposed cybercrime legislation.

Obstacles to Access

According to the International Telecommunication Union (ITU), Brazil had 68 million internet users as of December 2008, accounting for 35.2 percent of the population. A lack of infrastructure affects large segments of users, mainly in rural areas, and is the primary barrier to internet connectivity. Nevertheless, great improvements have been made in recent years as the government has initiated dozens of programs to connect the population to the internet, including investment in WiMax Networks and Digital Cities projects.[3] Many of these projects employ broadband technology, which is accessible to a majority of users. The internet is used by people at various socio-economic

[1] *Brazil Internet States and Telecom Market Report,* http://www.internetworldstats.com/sa/br.htm accessed on March 26, 2009
[2] "Hobbes' Internet Timeline v8.2", *Zakon Group LLC,* http://www.zakon.org/robert/internet/timeline/ accessed on March 26, 2009, and *The Brazilian Green Book on the Information Society* that brings the national backbone map: http://www.mct.gov.br/index.php/content/view/18878.html accessed om March 26, 2009 and http://www.rnp.br/backbone/index.php accessed on March 26, 2009
[3] "Neovia and Redline initiate US$30 million WiMAX network in Brazil", *WiMAX Industry*, August 2, 2007, http://www.wimax-industry.com/pr/7p.htm accessed on March 26, 2009; and http://www.teleco.com.br/cidadesdigitais.asp accessed on March 26, 2009

levels,[4] and the country's e-commerce, e-government, and online-banking services are among the most developed in the world.[5] However, due to persistent poverty, internet access remains out of reach for large portions of the population.

Six companies share the majority of the mobile-phone market, and penetration is increasing rapidly. Statistics show an average annual increase of 20 percent over the last five years and approximately 151 million mobile phones as of November 2008.[6]

While there have been no major cases of internet blocking by the executive branch, there were several incidents during the coverage period in which the judiciary interfered with access to certain online applications. In 2007, a judge ordered the removal of a video clip showing the private acts of a model and her boyfriend after the woman sued the YouTube video-sharing site.[7] YouTube attempted to comply, but users constantly reposted the offending video. The judge then requested that Brazilian internet service providers (ISPs) block the entire site. As a result, YouTube was inaccessible in Brazil for several days in January 2007. The decision was eventually reversed.[8]

Though they are generally accessible, Google's social-networking site Orkut and the blog service Wordpress have also been temporarily blocked following orders by the Brazilian judiciary and police. Such incidents have arisen in cases related to pedophilia, hate speech, and racist, homophobic, or defamatory material. Brazilian ISPs apparently lack the technical knowledge or software needed to block a single URL and are therefore forced to limit access to an entire site to comply with government requests. In some cases, however, alternative agreements have been reached between the judiciary and ISP companies to restrict access to the content in question.[9]

Despite an intricate regulatory environment, there are no specific legal or economic obstacles preventing the operation of diverse businesses that provide access to digital technologies. As a consequence of privatization plans implemented in the 1990s, however, the telecommunications market in general, and the ISP market in particular, tend toward concentration. More than 1,000 ISPs now operate in the country, according to the Brazilian Association of ISPs (ABRANET). However, the four largest companies—Terra, UOL, IG, and Yahoo!—hold more than 50 percent of the market. Broadband access is increasing as prices fall,[10] but it is also concentrated among telecommunications and cable companies.[11]

The telecommunications regulatory body, ANATEL, and the antitrust body, CADE, work to ensure that information and communication technologies (ICTs) operate in a free, fair, and independent manner, under the rule of law. These federal bodies have an interagency cooperation agreement defining concurrent competencies, and CADE is authorized by the General

---

[4] "In Brazil, Internet Access Grows Rapidly, Even Among Poor", *World Politics Review*, April 3, 2008, http://www.worldpoliticsreview.com/article.aspx?id=1891 accessed on March 26, 2009

[5] "Brazil-Internet and Broadband Market", *Research and Markets*, December 2008, http://www.researchandmarkets.com/reportinfo.asp?report_id=680153 accessed on March 26, 2009

[6] http://www.teleco.com.br/ncel.asp accessed on March 26, 2009

[7] "YouTube Does Brazil", *OpenNet Initiative*, January 10, 2007, http://opennet.net/blog/2007/01/youtube-does-brazil, accessed on March 26, 2009

[8] http://idgnow.uol.com.br/internet/2007/01/09/idgnoticia.2007-01-09.9436244203/IDGNoticia_view accessed on March 26, 2009 ; and "Brazil court revises ban on YouTube over sex video", *Reuters*, January 9, 2007 http://www.reuters.com/article/internetNews/idUSN0948365620070109 accessed on March 26, 2009 "YouTube wins Cicarelli (Brazilian model beach sex video) case", *Boing Boing*, June 27, 2007, http://www.boingboing.net/2007/06/27/youtube-wins-cicarel.html accessed on March 26, 2009

[9] "Brazil court orders ISPs to block access to Wordpress blog", *OpenNet Initiative*, April 10, 2008, http://opennet.net/blog/2008/04/brazil-court-orders-isps-block-access-wordpress-blog access on March 26, 2009

[10] "Broadband in Brazil Exceeds 8.1 Million Connections", *Cisco*, March 5, 2008, http://newsroom.cisco.com/dlls/2008/prod_030508b.html accessed on March 26, 2009

[11] http://www.teleco.com.br/blarga.asp Accessed on March 26, 2009

Telecommunications Law to have the final word when dealing with antitrust issues, such as market concentration and price setting.[12] In a pioneering initiative, the Brazilian Internet Steering Committee (CGI.br), a multi-stakeholder organization, was created in 1995 to guarantee transparency and social participation in issues related to internet governance.[13] Representatives from the government, the private sector, academia, and the nongovernmental organization (NGO) community sit as members, with the latter chosen since 2004 in relatively democratic and open elections.

Limits on Content

The government does not employ any technical methods to filter or otherwise limit access to online content. Nonetheless, legal action by the judiciary and government officials has emerged in recent years as a barrier to free speech and a means of removing content that is deemed undesirable. In December 2007, a court in the southern city of Porto Alegre forced journalist Vitor Vieira to withdraw content from an internet site that implicated a state representative.[14] In October 2008, an injunction was ordered against the Folha Online website, requiring it to remove a corruption-related report on Workers' Party candidate Luiz Marinho's alleged visit to a nightclub on automaker Volkswagen's tab.[15] In another incident in 2008, the opposition online journal *NovoJornal*, known for its criticism of Minas Gerais state governor Aecio Neves, was taken down by the authorities. They cited charges of posting anonymously, contrary to constitutional provisions that forbid anonymity; however, the website's director had reportedly registered the publication under his name as required by law.[16]

In a move that was seen as having a negative impact on the democratic process, restrictions were placed on the use of online applications for political campaigning during the 2008 elections. Resolution 22718, passed in March 2008 by the Superior Electoral Tribunal, determined that electoral campaigns and advertisements could only be posted on the candidates' web pages. It barred electoral campaigns from using such tools as Orkut, YouTube, e-mail, and SMS to circulate their political messages.[17] At least one case was reported in which a candidate in local elections was forced to close her Orkut account and suspend YouTube videos promoting her candidacy.[18] The

[12] "Reforms in Brazilian Telecommunications Regulations and their Impact on Sector Competition", *Global Competition Review,* http://www.globalcompetitionreview.com/reviews/9/sections/31/chapters/361/reforms-brazilian-telecommunications-regulations-impact-sector-competition accessed on March 26, 2009 and "Legislation Documents of the Telecommunications in Brazil", *Telesco*, http://www.teleco.com.br/en/en_legis.asp accessed on March 26, 2009

[13] *Brazilian Internet Steering Committee*, http://www.cg.org.br/internacional/index.htm accessed on March 26, 2009

[14] Freedom House, *Freedom of the Press 2008* Brazil country report

[15] "Electoral judge orders website to remove report on Worker's Party candidate", *IFEX*, October 22, 2008, www.ifex.org/en/content/view/full/97808/ accessed on 3/19/2009

[16] "Brazil: Inventive censorship, and the case for anonymity", *Global Voices*, September 7, 2008,http://globalvoicesonline.org/2008/09/07/brazil-inventive-censorship-and-the-case-for-anonymity/ accessed on March 26, 2009

[17]"Brazil: Blogs banned from the 2008 elections",*Global Voices*, March 30, 2008, http://globalvoicesonline.org/2008/03/30/brazil-blogs-banned-from-the-2008-elections/ accessed on March 26, 2009 and http://www.tse.gov.br/internet/index.html Accessed on March 26, 2009 and "Orkut Brazil warns users against political showdown regarding upcoming elections", *Orkut Plus*, September 14, 2008, http://www.orkutplus.net/2008/09/orkut-brazil-warns-users-against-political-showdown-regarding-upcoming-elections.html accessed on March 26, 2009

[18] "Brazil: Electoral censorship at work", *Global Voices*, July 22, 2009, http://globalvoicesonline.org/2008/07/22/brazil-electoral-censorship-at-work/ accessed on March 26, 2009

regulations also prohibited campaigns from buying advertising space on the internet. ISPs reportedly tried to overcome this resolution but were unsuccessful. In a related case, in July 2008 the Rio de Janeiro Regional Electoral Court demanded that bloggers delete banners they had displayed on their sites to support mayoral candidate Fernando Gabeira. After a public outcry, however, the judge reversed the decision the following day, reinforcing the interpretation that the regulations applied to campaigning by candidates themselves, rather than their supporters.[19]

There are generally no limitations on national or international news sources, and individuals are able to use the internet, mobile technology, and other ICTs as sources of information.[20] Blogs, photo-blogs, social-networking platforms, and citizen journalism have proliferated in recent years.[21] Over 80 percent of adult internet users visited social-networking sites in 2008, one of the highest such rates in the world.[22] While more and more Brazilians are using Facebook, Orkut remains the most popular of these platforms. Academic institutions have also begun using the internet to share information, presenting the results of scientific and academic research in online formats, adopting open-access strategies for many leading journals, and publishing public universities' theses and monographs. Another recent phenomenon has been the growing number of blogs written by policemen with the apparent intention of increasing transparency and building trust among the public.

The internet is widely used for social mobilization and campaigns. Examples include the Open and Free software movements, the AIDS and Access to Knowledge movement, and the gay rights movement. In addition, mobile phones have become a major tool for organizing events like the annual gay parade in Sao Paulo, as well as a means for distributing images related to violence in the country's streets. The internet has especially been used by the blogging community and others as a vehicle for protesting government policies and judicial decisions that are perceived as threats to online expression. Thousands of internet users launched an e-mail protest against the ban on YouTube, and a "No to the Ban" blog was created in response to concerns that the country's main blog-hosting platform, Wordpress, would be blocked by the courts.[23] An online petition in defense of free speech and against the proposed cybercrimes bill garnered 58,000 signatures in its first week.[24]

Violations of Users' Rights

While free speech is protected in the constitution, contradictory provisions and several legal rulings in favor of censorship during the coverage period have raised concerns that challenges to free

[19] "Brazil: First blog falls victim to electoral law", *Global Voices,* June 1, 2008, http://globalvoicesonline.org/2008/06/01/brazil-first-blog-falls-victim-to-electoral-law accessed on March 26, 2009

[20] *Brazil National Online Newspapers eNews Reference*, http://www.enewsreference.com/newspaper/brazina.htm accessed on March 26, 2009

[21] (Some top ranked Brazilian blogs can be seen here) http://colunistas.ig.com.br/metablog/2008/05/05/os-blogs-mais-acessados-do-brasil Accessed on March 26, 2009; and http://www.interney.net/?p=9760065 accessed on March 26, 2009; and "Eighty Five Percent of Brazilian Internet Users Visited a Social Networking Site in September 2008", *ComScore*, November 19, 2008, http://www.comscore.com/press/release.asp?press=2592 accessed on March 26, 2009

[22] "Eighty Five Percent of Brazilian Internet Users Visited a Social Networking Site in September 2008", http://www.comscore.com/press/release.asp?press=2592 accessed on March 26, 2009

[23]"Brazil: Bloggers united against Wordpress ban", *Global Voices*, April 12, 2008, http://advocacy.globalvoicesonline.org/2008/04/12/brazil-bloggers-united-against-wordpress-ban accessed on March 26, 2009

[24] http://www.petitiononline.com/veto2008/petition.html Accessed on March 26, 2009;and "Brazil: Bloggers question the 13 new cyber-crimes", *Global Voices*, July 17, 2008, http://globalvoicesonline.org/2008/07/17/brazil-bloggers-question-the-13-new-cyber-crimes/ accessed on March 26, 2009

expression affecting the traditional media may also be applied to online content. The constitution and federal law preserve freedom of speech as well as cultural and religious expression. Specific laws also establish freedom of the press. However, some legislation limits aspects of these rights, and the constitution outlines a particularly complex legal framework, especially regarding online speech.[25] For example, free expression of thought is assured and anonymity is formally forbidden in the same paragraph.[26]

Civil and administrative charges against ISPs, online news journals, and some bloggers have become regular occurrences in the judicial system in recent years.[27] In addition to the cases mentioned above, Google Brazil and some of its services, such as Orkut and YouTube, have been the target of numerous judicial demands. In one incident, Google was required to take down Orkut communities that were seen as offensive to Edir Macedo, an evangelical minister.[28] Actress Preta Gil sued the company for linking her with the term "fat actress," and in another case Google Brazil was ordered to compensate a woman after she was called a "deadbeat" on Orkut. The popular networking site has also been penalized for allowing fake profiles; a lawyer from Santa Catarina state was arrested for using such a profile. The authorities have threatened in the past to block access to the Wordpress blogging site, a result of their inability to censor specific web addresses.[29]

Individual bloggers have also faced lawsuits by politicians. More than 25 defamation suits have been brought against blogger Alcinea Cavalcanti, the majority of them initiated by Senator Jose Sarney, who felt personally offended by the content of several postings.[30] Such official use of the courts to silence critics was discussed during a recent public hearing of the Inter-American Commission on Human Rights at the Organization of American States (OAS). The Brazilian Association of Investigative Journalism (ABRAJI) called on the commission to review the laws and judicial practices that violate freedom of expression in Brazil; any ruling on the issue by the commission would affect both traditional and online media.[31]

An ongoing concern for freedom of expression advocates in the country has been the cybercrimes bill,[32] which was first introduced in 2006 by Senator Eduardo Azeredo.[33] Following pressure from the public, certain provisions that were included in the initial version, such as requirements for user registration, have reportedly been dropped. Nevertheless, the bill in its current form would still restrict technologies like open wi-fi networks and oblige ISPs to record user

---

[25] "Constitution of Brazil", *Brazil Information*, http://www.v-brazil.com/government/laws/constitution.html Accessed on March 26, 2009

[26] "Brazil: Inventive censorship, and the case for anonymity", http://globalvoicesonline.org/2008/09/07/brazil-inventive-censorship-and-the-case-for-anonymity accessed on March 26, 2009

[27] For more information see:http://globalvoicesonline.org/found/?cof=FORID%3A9&q=Brazil+and+Internet+Freedom&btnG=Search+%C2%BB&cx=000932313665553177304%3Adg67ra11mvs#1039 accessed on March 26, 2009

[28] http://www.htmlstaff.org/ver.php?id=15748 accessed on March 26, 2009

[29] "Brazil: Bloggers united against Wordpress ban", http://advocacy.globalvoicesonline.org/2008/04/12/brazil-bloggers-united-against-wordpress-ban accessed on 3/19/2009

[30] FotP Brazil (2008)

[31] "Press release on OAS hearing", *ABRAJI*, November 11, 2008, http://www.abraji.org.br/?id=90&id_noticia=612 ; and http://knightcenter.utexas.edu/site_search.php?keyword=Brazil accessed on March 26, 2009

[32] "Censura Não!: Brazilian Bloggers Protest New Cybercrime Bill", *OpenNet Initiative*, July 25, 2008, http://opennet.net/blog/2008/07/censura-n%C3%A3o-brazilian-bloggers-protest-new-cybercrime-bill ; and "Legislators urged to oppose cyber-crime bill likely to threaten online free expression", *Reporters Without Borders*, July 23, 2008, http://www.rsf.org/article.php3?id_article=27917 accessed on March 26, 2009

[33] "Brazil: Bloggers question the 13 new cyber-crimes",http://globalvoicesonline.org/2008/07/17/brazil-bloggers-question-the-13-new-cyber-crimes/ accessed on March 26, 2009; and "Brazilian Cybercrime bill needs more transparency", *Safernet Brasil*, June 17, 2007, http://www.safernet.org.br/site/noticias/brazilian-cybercrime-bill-needs-more-transparency accessed on March 26, 2009

information and keep it for three years. It also allows providers to check for copyright infringements in data sent via peer-to-peer connections, along with other threats to users' right to privacy.[34] Ronaldo Lemos, director of the Center for Technology & Society at the Fundação Getulio Vargas (FGV) Law School, has raised concerns over the text's vagueness, its unpredictable consequences, and the possibility that if it is passed, users could be criminally liable for trivial actions conducted over the internet and punishable with prison terms as long as four years.[35] In July 2008 the Senate passed the bill, which then went to the House of Representatives, where it remained at year's end.

Surveillance of internet activities is not a significant concern in Brazil. Specific laws allow for surveillance, but only when authorized by judicial orders under due process. Nevertheless, surveillance of telephones, including mobile phones, has reportedly been used more extensively in recent years. In 2007, the number of wiretaps was estimated at between 300,000 and 409,000, and most were apparently carried out without a judicial order.[36] In addition, the Federal Police and a private software company developed a wiretapping system called Guardião (Guardian). This system was criticized after the disclosure of some of its capabilities, such as the remote and automated monitoring of up to 3,000 telephone lines, whether fixed and mobile.[37]

While traditional media workers are often victims of violence and death threats in Brazil, such attacks have yet to extend significantly to online journalists, bloggers, and commentators.[38] Nonetheless, bloggers who report on police corruption and related issues are targeted from time to time, and the overall environment of intimidation contributes to self-censorship among them. Average users express themselves quite freely.

[34] "Access versus surveillance: Brazilian cybercrime law project" , *iCommons*, November 5, 2008, http://icommons.org/articles/access-versus-surveillance-brazilian-cybercrime-law-project accessed on March 26, 2009
[35] http://a2kbrasil.org.br/Esclareca-suas-Duvidas-sobre-os
[36] http://www.conjur.com.br/static/text/60835,1 accessed on March 26, 2009; and http://www.fecomercio.com.br/pagina.php?tipo=21&pg=675 accessed on March 26, 2009
[37] http://www2.oabsp.org.br/asp/jornal/materias.asp?edicao=113&pagina=3117&tds=7&sub=0&sub2=0&pgNovo=67 accessed on March 26, 2009
[38] FotP Brazil (2008).

China

Status: Not Free

Obstacles to Access: **18** (0–25)
Limits on Content: **27** (0–35)
Violations of User Rights: **33** (0–40)
Total Score: **78** (0–100)

Population: 1.3 billion
Internet Users/Penetration 2006: 137 million / 10 percent
Internet Users/Penetration 2008: 298 million / 22 percent
Mobile Phone Users/Penetration 2006: 461 Million
Mobile Phone Users/Penetration 2008: 633 Million
Freedom of the Press (2008) Score/Status: 84 / Not Free
Digital Opportunity Index (2006) Ranking: 77 out of 181
GNI Per Capita (PPP): $5,400
Web 2.0 Applications Blocked: Yes
Political Content Systematically Filtered: Yes
Bloggers/Online Journalists Arrested: Yes

Introduction

Although China is home to the largest population of internet users in the world and has witnessed increasing creativity and "pushback" from its netizens, the country's internet environment remains one of the most controlled in the world. China's 1.3 billion citizens have only a limited ability to access and circulate information that is vital to their well-being and the country's future direction. The Chinese authorities maintain a sophisticated and multilayered system of mechanisms for censoring, monitoring, and controlling activities on the internet and mobile telephones. This system has been enhanced in recent years with new attempts to manipulate online discussion, including the recruitment of commentators to guide opinions and more forceful encouragement of self-discipline among private internet companies and web-hosting services. The country also boasts the world's largest number of individuals imprisoned for their online activities, with at least 49 cyberdissidents behind bars as of mid-2008.[1]

The internet was first opened for public access in China in 1996, and the number of users has since grown exponentially, from 20 million in 2001 to over 200 million in 2008.[2] From the beginning, however, the Chinese government has sought to assert its authority over the new medium. The underlying system of infrastructural control and filtering technology has been more or less complete since 2003,[3] while more sophisticated forms of content manipulation have gained prominence only recently. Nevertheless, due to the egalitarian nature and technical flexibility of the internet, the online environment remains more free than traditional media. In recent years, the country's growing community of bloggers, online commentators, and human rights defenders has played a role in uncovering official corruption, mobilizing citizens for humanitarian efforts, and exposing rights abuses. Some groups have used information and communication technologies (ICTs) to launch more direct critiques of the regime, though the authorities have thus far managed to prevent a viable alternative to the current political system from gaining momentum in cyberspace.

[1] "Cyber-dissident accused of illegal possession of state secrets is denied right to see lawyer", Reporters without Borders, July 21, 2008, http://www.rsf.org/article.php3?id_article=27892 Accessed on 3/23/2009
[2] China Internet Network Information Center (CNNIC), http://www.cnnic.cn/html/Dir/2003/10/22/1001.htm Accessed on 3/23/2009
[3] http://www.people.com.cn/GB/it/53/142/20030226/931430.html Accessed on 3/23/2009

Obstacles to Access

Realizing the potential contributions of the internet and other ICTs to economic modernization and growth, the Chinese leadership has encouraged the expansion of the necessary infrastructure. Obstacles to access remain, however, including an urban-rural divide, restricted access to advanced applications, government control over the backbone of the network, and a freeze on the opening of new cybercafes.

In 2008, China surpassed the United States as home to the largest number of internet users in the world, with the government-linked China Internet Network Information Center (CINIC) announcing a total of 298 million users.[4] Given the total size of the country's population, however, the overall penetration rate is just 22.6 percent, a low figure by global standards. Moreover, rural users account for only 28 percent of the total, according to CNNIC.[5] While most users access the internet from home or work, an estimated 40 percent use cybercafes, particularly those with lower incomes.[6] Broadband access is widespread. Use of mobile telephones has also spread quickly. According to the ITU there were 633 million mobile-phone users in China by the end of 2008,[7] giving the country a penetration rate of nearly 50 percent and the world's largest population of mobile users.[8] Access to the internet via mobile phones has increased in recent years; state-run media reported that 117 million people used this service in 2008, more than double the total from the previous year.[9] The increase in both the overall internet population and the number of mobile internet users may be attributed in part to a gradual decrease in the cost of broadband and mobile-phone access.

There is widespread access to internet technology and applications, such as video-sharing websites, social-networking tools, and e-mail services, but extensive restrictions remain, particularly on advanced applications whose providers are based outside the country. The YouTube video-sharing site and overseas blogging platforms like Wordpress and Blogspot cannot be accessed reliably in China; the e-mail services Gmail and Hotmail are frequently jammed. The social-networking site Facebook, which is popular among Chinese college students, was periodically blocked during 2008, especially during the run-up to the Beijing Olympics.[10] In cases where international applications are available, as with Google search engines and Skype Voice over Internet Protocol (VoIP), the foreign corporations in question have agreed to alter their services and implement monitoring and censorship of political content in order to gain access to the market.[11] For international applications that remain blocked, Chinese equivalents have emerged and gained immense popularity, though they are more susceptible to government control. In 2007, the State Administration of Radio, Film, and Television (SARFT), which oversees audiovisual content on the

[4] ITU, http://www.itu.int/ITU-D/icteye/Default.aspx Accessed on 3/23/2009;
and http://www.cnnic.cn/uploadfiles/doc/2009/1/13/92209.doc Accessed on 3/23/2009
[5] http://www.cnnic.cn/uploadfiles/doc/2009/1/13/92209.doc Accessed on 3/23/2009
[6] http://www.cnnic.cn/uploadfiles/doc/2009/1/13/92209.doc (p27) Accessed on 3/23/2009
[7] ITU, http://www.itu.int/ITU-D/icteye/Default.aspx, the Ministry of Industry and Information Technology (MIIT) puts the number at 641 million
[8] http://www.miit.gov.cn/n11293472/n11295057/n11298508/11912660.html Accessed on 3/23/2009
[9] "117m Chinese surf Internet via mobile phones, up 113% *", China Daily,* January 13, 2009, www.chinadaily.com.cn/bizchina/2009-01/13/content_7392583.htm Accessed on 3/23/2009
[10] "Aw on the Internet" blog, http://www.awflasher.com/blog/archives/1354 Accessed on 3/23/2009
[11] "Google founder admits compromise over China", *The Scotsman,* June 8, 2006, http://edinburghnews.scotsman.com/google/Google-founder-admits-compromises-over.2782379.jp Accessed on 3/23/2009;
and "China Skype services snags and stores users' messages", *The Register,* October 2, 2008, www.theregister.co.uk/2008/10/02/skype_surveillance_in_china/ Accessed on 3/23/2009

internet, ordered that all video-sharing websites must be state owned, except for several large examples that had already become influential.[12] SARFT subsequently shut down many video-sharing sites and demanded that the three major ones—Tudou.com, 56.com, and Youku.com—be closed for several days in 2008 to conduct a "self-inspection" and ensure that adequate content controls were in place.[13] In some instances, the government has shut down access to ICTs or applications surrounding specific events. During the summer and fall of 2007, prior to the 17th Party Congress, the authorities carried out a widespread shutdown of data centers housing servers for websites, online bulletin boards, and comment forums, affecting millions of users.[14] Similarly, following unrest in Tibet in March 2008, the government attempted to control the flow of information to and from the region, disrupting mobile-phone service there and blocking YouTube across China.[15] Major circumvention websites like anonymizer.com and proxify.com have also been blocked, while more sophisticated tools like Freegate and TOR are closely monitored and frequently attacked by the authorities.

Internet access was once monopolized by China Telecom, but recent waves of reform have liberalized and decentralized ownership of internet-service providers (ISPs) in the country, making the system less strict than that of traditional media. Users can now opt to access the internet through private ISPs, among which the Great Wall Broadband Network is the most popular broadband provider in major cities. A license from the MIIT is required to establish an ISP or host a website within China, though approval has recently become easier to obtain than in the past.

The government has been willing to liberalize the ISP market in part because of the centralization of the country's connection to the international internet, which is controlled by six to eight state-run operators that maintain advanced international gateways in Beijing, Shanghai, and Guangzhou.[16] This arrangement remains the primary infrastructural limitation on open internet access in the country. According to regulations issued by the MIIT, a commercial ISP can function only when it subscribes to the gateway operators. Moreover, the MIIT can revoke the license of any ISP that fails to comply with its regulations and orders. This network design essentially creates a national intranet and gives the authorities the ability to cut off any cross-border information requests that are deemed undesirable.

The authorities have also sought to exercise fairly tight control over cybercafes, which would otherwise enable anonymous communication and networking among citizens. The issuance of licenses for the establishment of cybercafes is managed by the Ministry of Culture (MC) and its local departments. The ministry has stepped up its regulation of cybercafes in recent years. In 2003, it ordered that the facilities must be operated as chain stores,[17] and since March 2007 it has indefinitely suspended the issuance of new licenses (there were 113,000 cybercafes in existence at the time).[18] Mobile-telephone communication is dominated by three state-owned operators: China Mobile,

[12] http://tech.163.com/08/0205/02/43TG2FVB000915BF.html Accessed on 3/23/2009
[13] "'Chinese YouTube' shutdown amid censor fears", *The Times Online (London),* June 20, 2008, http://technology.timesonline.co.uk/tol/news/tech_and_web/article4179103.ece Accessed on 3/23/2009 and "China softens rules on video-sharing websites", *Los Angeles Times,* February 6, 2008 http://articles.latimes.com/2008/feb/06/world/fg-video6 Accessed on 3/23/2009
[14] "Attacks on Press 2007: China", Committee to Protect Journalists, http://www.cpj.org/2008/02/attacks-on-the-press-2007-china.php Accessed on 3/23/3009
[15] "China blocks YouTube, Yahoo! over Tibet", *The Times Online (London),* March 17, 2008, http://technology.timesonline.co.uk/tol/news/tech_and_web/article3568040.ece Accessed on 3/23/3009
[16] CNNIC, http://www.cnnic.cn/uploadfiles/doc/2009/1/13/92209.doc Accessed on 3/23/3009
[17] http://www.linkwan.com/gb/news/html/4186.htm Accessed on 3/23/2009
[18] "2008 *Freedom of the Press* report on China", Freedom House , http://www.freedomhouse.org/template.cfm?page=251&country=7372&year=2008 Accessed on 3/23/2009

China Telecom, and China Unicom.[19] Under the oversight of the MIIT, connection to the internet via mobile phones is also monitored by the international gateway operators.

Limits on Content

The Chinese authorities employ a wide range of mechanisms at every layer of communication to limit free expression online and control the flow of information via ICTs. At the same time, the Chinese blogosphere is active and creative, and a growing number of netizens use ICTs to spread information and opinions. Thus far, the authorities have managed to prevent this from translating into open political opposition to Communist Party rule or a groundswell of public criticism of the government's key policies.

The Communist Party's internet control strategy consists of four different techniques: technical filtering, prepublication censorship, postpublication censorship, and proactive manipulation. While the first is primarily aimed at content based outside of China, the latter three apply to content produced and posted within China as well. The purported goal is to limit the spread of pornography, gambling, and other harmful practices, but such content is generally easier to access than information related to political and religious groups, human rights violations, and alternative news sources.[20] The most systematically censored topics are those deemed by the Communist Party to be the most threatening to its domestic legitimacy. These include criticism of top leaders, independent evaluations of China's rights record, violations of minority rights in Tibet and Xinjiang, the Falun Gong spiritual group, the 1989 Beijing massacre, and various dissident initiatives that challenge the regime on a systemic level, such as the Nine Commentaries (a series of editorials analyzing the history of the party and encouraging an end to its rule) and more recently Charter 08 (a prodemocracy manifesto calling for a multiparty system).[21] These standing taboos are supplemented regularly by directives and terms targeting specific, unforeseen incidents and other events about which the government wishes to suppress news or opinions, such as the work of individual human rights defenders, allegations of shoddy construction surrounding the Sichuan earthquake, occurrences related to the Olympics, antigovernment riots in various localities, and indeed any references to censorship. Broader politically oriented terms such as "democracy," "human rights," and "freedom of speech" are subject to less extensive censorship.[22]

Technical Filtering: Restricting access to foreign websites is a key component of technical filtering, enabled by the channeling of all internet traffic through the gateway operators described above. Among the websites that are systematically blocked are those of political parties in Taiwan or groups supporting greater freedom for religious and ethnic minorities; human rights organizations like Amnesty International, Freedom House, and Human Rights Watch; news outlets like the Hong Kong–based *Apple Daily*, the British Broadcasting Corporation (BBC) Chinese service, and Radio

[19] According to the WTO agreements, the share taken by foreign capital in the telecom operators can't exceed 49%. See, http://www.shjubao.cn/epublish/gb/paper22/1/class002200036/hwz532030.htm Accessed on 3/23/2009

[20]"Censorship in Chinese Media", *New York Times,* September 25, 2008 http://economix.blogs.nytimes.com/2008/09/25/censorship-in-chinese-media/ Accessed on 3/23/2009

[21] Graph from Open Net Initiative 2005 study of filtering in China, available through "Written evidence submitted by Sarah Cook, Student at the School of Oriental and African Studies, University of London", House of Commons, http://www.publications.parliament.uk/pa/cm200607/cmselect/cmfaff/269/269we08.htm Accessed on 3/23/2009; and "Breaching Trust", International Warfare Monitor ONI Asia, October 1, 2008, http://www.nartv.org/mirror/breachingtrust.pdf Accessed on 3/23/2009; and "Charter 08: Why it should be called Wang",*Chinayourren.com*, January 11, 2009 http://chinayouren.com/eng/2009/01/charter-08-why-it-should-be-called-wang/ Accessed on 3/23/2009

[22] See note 20.

Free Asia; and overseas dissident publications. In 2008, the government's pledges of unfettered internet access for foreign journalists during the Olympics were not upheld; although a number of previously censored sites were unblocked following an international outcry, sites related to Tibet or the Falun Gong remained blocked as usual throughout the games.[23] Similarly, while some foreign sites were unblocked for Chinese users before the opening ceremony of the Beijing Olympics, most of them were inaccessible again by late 2008.[24] In addition to blocking entire websites, the sophisticated technology employed by the authorities enables the filtering of particular pages within sites that are otherwise approved, if the pages are found to contain blacklisted keywords in the URL path. Filtering by keyword is also implemented in instant-messaging services, such as Tom-Skype and QQ, and the necessary software is built into the application upon installation.[25]

Prepublication censorship: Prepublication censorship is enforced using lists of taboo topics, which Chinese government bodies, mainly the Information Office of Beijing (or its equivalent in other cities), periodically issue as circumstances require. These are accompanied by specific instructions on how to treat the proscribed topics, such as not placing certain content in an important position on a homepage, not allowing it to appear in blog entries and comment forums, or not reprinting items from foreign news sources. Such orders are expected to be carried out—either automatically or manually—by state-run online news outlets and private companies running a wide variety of websites; the latter risk losing their business licenses if they fail to comply. Most postings on blogs, comment sections of news items, and bulletin board system (BBS) discussions that are deemed objectionable are deleted at this stage. Tests conducted recently found that entries containing sensitive keywords such as "June 4," "Falun Gong," or "Dalai Lama" could not be displayed on Chinese blog hosting services, including the simplified Chinese version of Microsoft's MSN Space Live service and Skype's Chinese version, Tom. A more extensive academic study found that while this practice was common, implementation was nonetheless inconsistent across blog hosting companies, and some potentially sensitive discussions did take place, indicating a tendency among private actors to resist government orders.[26] In an additional form of prepublication censorship that has been used in some localities, a system of virtual internet policing employs the animated characters "Jing Jing" and "Cha Cha" to warn users of online content infringements.

Postpublication censorship: Postpublication censorship, applied to information that has already been posted, can take a number of forms. Individual blog entries may be deleted, in most instances within 24 to 48 hours of their posting. In other cases, entire blogs may be shut down by service providers, as has occurred with several well-known bloggers in recent years.[27] In addition, search engines including the China versions of Google and Yahoo! filter results to exclude those that do not favor the Chinese authorities' perspective. Since e-mail messages circulated within the country cannot be filtered at the international gateways, service providers have been pressured to carry out their own censorship; many have reportedly complied, including the popular Sohu and QQ.

---

[23] "Web curbs for Olympic journalists", BBC News, July 30, 2008, http://news.bbc.co.uk/2/hi/asia-pacific/7532338.stm Accessed on 3/23/2009 and "Internet censorship plagues journalists at the Olympics", *Cnet.com*, July 29, 2008, http://news.cnet.com/8301-1023_3-10002097-93.html Accessed on 3/23/2009

[24] "Post-Olympic China Olympic China turns its back on Internet censorship promises",*DailyTech,* December 18, 2008, www.dailytech.com/PostOlympics%2BChina%2BTurns%2BIts%2BBack%2Bon%2BInternet%2BCensorship%2BPromises/article13716.htm Accessed on 3/23/2009

[25] "A list of censored words in Chinese cyberspace", *China Digital Times,* http://chinadigitaltimes.net/2004/08/the-words-you-never-see-in-chinese-cyberspace/ Accessed on 3/23/2009

[26] "China's censorship 2.0: How companies censor bloggers", *First Monday,* February 2, 2009, http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2378/2089 Accessed on 3/23/2009

[27] http://inmediahk.net/node/1001868 Accessed November-December 2008

Proactive manipulation: In addition to preventing certain content from appearing in Chinese cyberspace, and partly in response to the growing prominence of the internet in shaping public perceptions, the Chinese authorities in recent years have introduced measures to proactively sway public opinion online and amplify the party's version of events over alternative accounts. Since 2005, paid web commentators known as "50 Cent Party" members or "Red Vests" have been recruited by the authorities to post progovernment remarks, lead online discussions along the party line, and report users who have posted offending statements.[28] Some estimates place the number of these commentators at over 250,000.[29] In other instances, such as the 2008 unrest in Tibet, censorship of unofficial accounts or deletion of critical comments has been combined with the required posting of the Xinhua news agency's articles, which enables the official version to dominate public discourse.[30]

A wide variety of government agencies at both the local and national level are involved in online content censorship. While the Propaganda Department of the Central Committee of the Chinese Communist Party (CPD) plays a key role in outlining topics for censorship, the Information Office of the State Council (IOSC), the MIIT, and the Ministry of Public Security (MPS) are the primary enforcement agencies. The IOSC mainly oversees online news content. The MIIT, the top technical authority, supervises the telecommunication infrastructure (for the internet as well as mobile phones), grants or revokes the licenses of private enterprises, and oversees the various technical censorship systems, including the international gateways and SMS (text message) jamming. The MPS has the power to track, investigate, and arrest users; monitor websites; and punish cybercafe owners.

In addition to the IOSC's oversight, online news is subject to aspects of the same regulatory system that applies to traditional media. Thus the General Administration of Press and Publication (GAPP) extends its core jurisdiction over printed media to relevant online publications. In other instances, specific bodies have been created to regulate internet content, such as the Internet Review Group, which operates within the CPD to inspect and monitor online material.[31] More recently, branches of the Administrative Office of Internet Propaganda (AOIP) under the direct control of provincial or municipal governments have been playing an increasingly active role in regulating the internet.[32]

[28] "Internet society of China wants people to report illegal and inappropriate content", *Passingnotes.com,* June 11, 2004, http://www.passingnotes.com/archives/2004/06/14/interfax-internet-society-of-china-wants-people-to-report-illegal-and-inappropriate-content/ Accessed on 3/23/2009 and http://www.ddgx.cn/news/2008/0730/index_tstt/091704.htm Accessed on 3/23/2009 and http://www.hhubbs.com/thread-64753-1-2.html Accessed on 3/23/2009

[29] "China's guerilla war for the web", *Far Eastern Economic Review,* July 2008, http://www.feer.com/essays/2008/august/chinas-guerrilla-war-for-the-web Accessed on 3/23/2009

[30] "China blacks out Tibet news", *Business Week,* March 17, 2008, http://www.businessweek.com/globalbiz/content/mar2008/gb20080317_321446.htm Accessed on 3/23/2009

[31] http://blog1.poco.cn/myBlogDetail.htx&id=328024&userid=4304898&pri=&n=0 Accessed on 3/23/2009

[32] "Internet censorship tightens in China ahead of Olympics", *Interfax.cn,* July 25, 2008, http://www.interfax.cn/news/4327/ Accessed on 3/23/2009

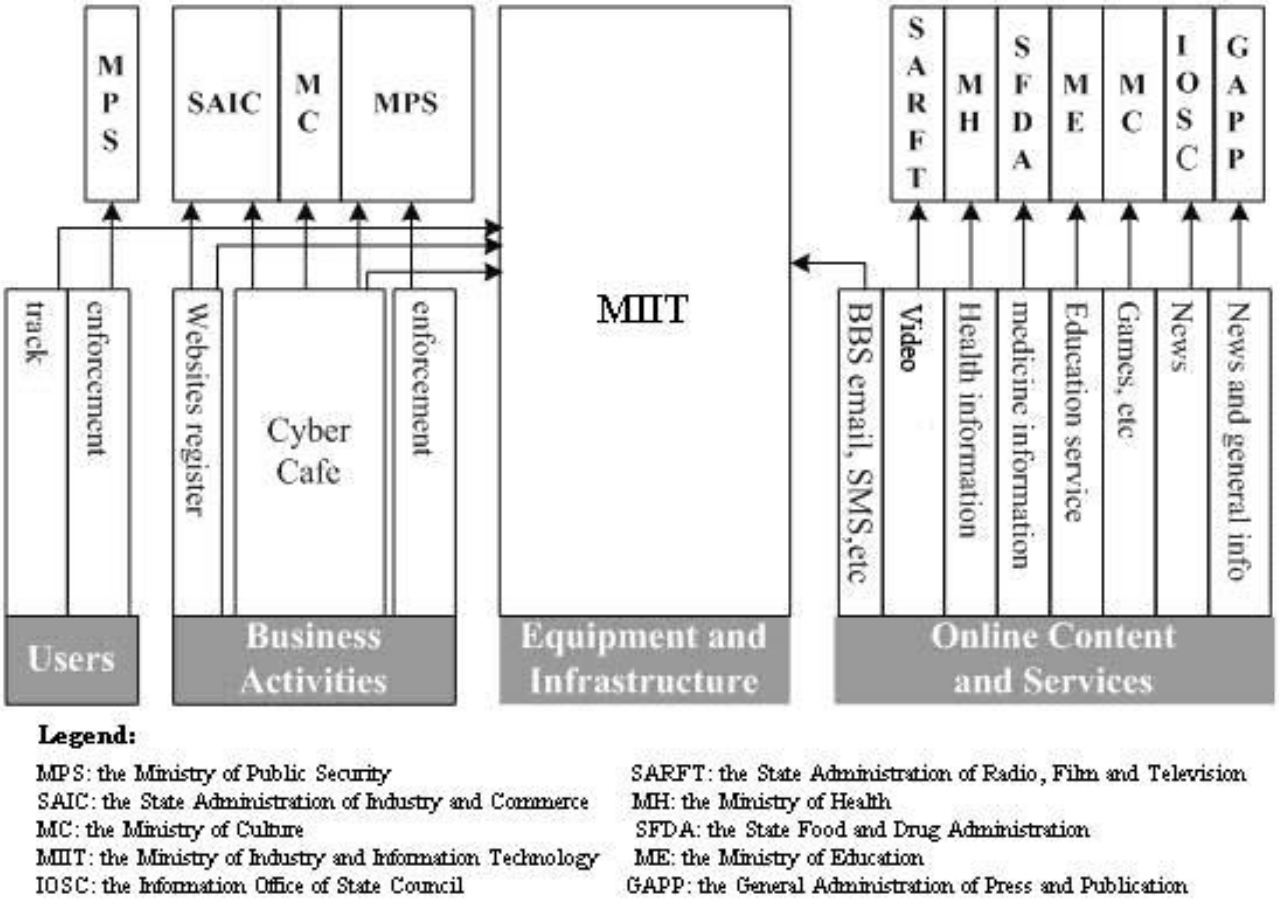


Figure 1: State Agencies Involved in Internet Control in China

Censorship decisions are largely nontransparent, though some private companies are known to alert readers that content has been removed for unspecified reasons. No avenue exists for appealing censorship decisions. In 2007, Chinese blogger and lawyer Liu Xiaoyuan attempted to sue Sohu for deleting his postings, arguing that it contravened the user terms of agreement, but the case was dismissed by a Beijing court.[33] Realizing the comprehensive nature of surveillance and censorship on the internet and SMS, ordinary users and bloggers engage in extensive self-censorship and often refrain from transmitting sensitive comments online or via mobile phones, particularly when anonymity is not ensured.[34]

Despite the multiple layers of control, the internet has emerged in recent years as a primary source of news and a forum for discussion for many Chinese, particularly among the younger generation. Indeed, a recent academic study estimated that there were approximately 72 million blogs in China at the end of 2007, along with nearly 17 million "active" bloggers updating their websites a minimum of one time per month.[35] Through this and other avenues, Chinese cyberspace

[33] "China's Internet controls tightened ahead of sensitive political congress", *Associated Press*, October 11, 2007, www.iht.com/articles/ap/2007/10/12/business/AS-FEA-TEC-China-Internet-Controls.php Accessed on 3/23/2009
[34] http://info.codepub.com/2007/06/info-15288.html Accessed on 3/23/2009 and http://news.163.com/06/1204/09/31G4P3CK00011SM9.html Accessed on 3/23/20009
[35] "Political Expression in the Chinese Blogosphere: Below the Radar," *Asian Survey,* September/October 2008, http://caliber.ucpress.net/doi/abs/10.1525/AS.2008.48.5.752 Accessed on 3/23/2009.

has grown into a dynamic environment, replete with online auctions, social networks, homemade music videos, a large virtual gaming population, and spirited discussion of some social and political issues. The latter discussions sometimes include the creative use of asterisks, code words, or homophones to replace potentially sensitive keywords. For example, censorship is referred to as "harmonization," and the 1989 massacre in Beijing, which involved the use of tanks, is described as "tractors coming into the city."[36] Many well-educated and web-savvy Chinese are able to bypass the government's control using a variety of technical circumvention tools. These individuals can thus obtain more information from overseas sources than the average citizen, and can act as opinion leaders in online discussions, particularly if they have knowledge of a foreign language.

The relationship between online journalism and traditional media is mutually reinforcing, primarily with respect to a small number of daring, investigative print publications. In several instances during the coverage period, traditional media outlets received tips or discovered sources online, reported on the information in commercial print publications, and thus generated further online discussion. Nevertheless, blogs and other internet platforms remain more likely than traditional media to contain criticism of the government and a broad spectrum of views.

Civil society organizations involved in education, health care, and other social and cultural issues that are deemed acceptable by the authorities often have an online presence. ICTs played a particularly prominent role in the aftermath of the Sichuan earthquake in May 2008, as people on the ground transmitted updates via Twitter and BBS comments, netizens created personalized videos and memorials, blogs became a platform for public sharing of memories, and millions of dollars were donated toward relief efforts via websites.[37] In some instances, the internet and SMS have been used to mobilize "real life" protests, as occurred in the southern city of Xiamen in 2007, when bloggers supported large-scale street protests that eventually succeeded in terminating the construction of a chemical factory nearby. In other cases, they have been used to circumvent government cover-ups or expose official malfeasance. SMS was employed to circulate epidemic information during the SARS outbreak in 2003,[38] and there were several cases in 2008 of internet users revealing acts of corruption by local officials, leading to their dismissal.[39] ICTs have also featured in the organization and venting of acute nationalist sentiment, initially with tacit government approval; prominent examples include the country's periodic anti-Japanese protests and the retribution against French companies after demonstrators in Paris disrupted the 2008 Olympic torch relay.[40]

In spite of the booming internet population and the skyrocketing number of websites, fully independent civil society, ethnic, and religious organizations remain underrepresented, though they have been able to use some ICTs to advance their causes. A loose network of lawyers, legal academics, and activists known as the *weiquan* or "rights defense" movement has used internet, e-mail, VoIP, and mobile-phone technology to circulate and publish open letters, document accounts of abuse, and organize a 2006 national relay hunger strike for human rights. More recently, in

[36] "China's web censors delete blogs, unplug servers", *Associated Press,* October 15, 2007, http://www.foxnews.com/story/0,2933,301488,00.html Accessed on 3/23/2009

[37] "Sichuan earthquake special edition" , *Slideshare,net,* Mary 27, 2008, http://www.slideshare.net/jason.zhanjia/iwom-watch-sichuan-earthquake-special-edition-presentation Accessed on 3/23/2009

[38] http://www.51friend.net/bbs/2290965mp1.aspx Accessed on 3/23/2009 Accessed on 3/23/2009 and "Breaking down the great firewall", BBC News, April 30, 2005, http://news.bbc.co.uk/2/hi/asia-pacific/4496163.stm Accessed on 3/23/2009

[39] "Two Steps Forward, One Step Back? A Review Of The Chinese Internet In 2008", *EastSouthWestNorth,* January 21, 2009, http://zonaeuropa.com/20090124_1.htm Accessed on 3/23/3009

[40] "Chinese nationalism fuels Tibet crackdown", *New York Times,* March 31, 2008, www.nytimes.com/2008/03/31/world/asia/31china.html?pagewanted=print Accessed on 3/23/2009

December 2008, a broad coalition of 300 such individuals issued a bold manifesto dubbed Charter 08, which called for significant political reforms including multiparty democracy, a free press, and an independent judiciary. Though the government suppressed broad public discussion of the proposal online, the initiative did circulate to a limited audience, garnering an additional 7,000 signatures.[41] Similarly, after being driven underground by a violent persecutory campaign, adherents of the Falun Gong spiritual practice have made use of the internet and mobile phones to maintain contact with one another, communicate with overseas practitioners, send documentation of torture abroad, and download censored information for the purposes of producing offline leaflets and DVDs that expose rights violations and call party propaganda into question. Meanwhile, overseas groups such as Radio Free Asia, Human Rights in China, and the *Epoch Times* have reportedly sent millions of e-mails into the country, supplying users with news summaries on Chinese and international events, instructions on anticensorship technology, and copies of banned publications like the Nine Commentaries.[42]

Violations of Users' Rights

Those who violate party directives on censorship or publish information on taboo topics face a range of possible sanctions, including criminal and financial liability, long terms of imprisonment, and loss of a business license, though enforcement is selective. Article 35 of the constitution guarantees the freedoms of speech, assembly, association, and publication, but such provisions are subordinated to the national interest. In addition, the constitution cannot be invoked in courts as a legal basis for asserting rights. The judiciary is not independent and closely follows party directives, particularly in politically sensitive freedom of expression cases. Although no legislation exists at the national level to clearly regulate online communication and indicate what ICT content is prohibited, a wide variety of regulations have been issued by different government agencies to establish censorship guidelines. A total of 81 ordinances involving 29 government agencies were issued between 1993 and 2007 to articulate various controls on content and communication over the internet.

In addition to internet-specific regulations, vague provisions in the criminal code and state-secrets legislation have been used to imprison citizens for their online activities, including publication of articles criticizing the government or exposing rights abuses, transmission of objectionable e-mail messages, and downloading of censored material from overseas websites. Hu Jia, a well-known human rights activist and winner of the European Sakharov Prize for Freedom of Thought, was sentenced to three and a half years in prison in April 2008 for "inciting subversion of state power" on the basis of several articles he had written and published online.[43] Other individuals detained or sentenced on such charges in recent years include writer Du Daobin,[44] professor Guo Quan,[45] lawyer Gao Zhisheng,[46] and most recently, freelance journalist Chen Daojun for his writings

[41] "Chinese Authorities Continue to Suppress *Charter 08*; Number of Signers Exceeds 7,200 ", *Human Rights in China*, January 9, 2009, http://www.hrichina.org/public/contents/press?revision_id=109512&item_id=107728 Accessed on 3/23/2009 and "Charter 08 Still Alive in the Chinese Blogosphere" *China Digital Times,* February 9, 2009,*http://chinadigitaltimes.net/2009/02/charter-08-still-alive-in-the-chinese-blogosphere/* Accessed on 3/23/2009

[42] *Mass Mailing*, http://us.dongtaiwang.com/dmirror/http/www.dit-inc.us/mass_mailing Accessed on 3/23/2009

[43] "Expression=prison: Hu Jia", *Amnesty International*, April 4, 2008, www.amnesty.org.au/china/comments/11747/ Accessed on 3/23/2009

[44] *Reporters Without Borders*, http://www.rsf.org/rubrique.php3?id_rubrique=119 Accessed on 3/23/2009

[45] "Blogger charged with subversion", *Radio Free Asia*, December 22, 2008, www.rfa.org/english/news/china/guoquan-12222008104700.html Accessed on 3/23/2009

expressing support for protesters in Tibetan areas in March 2008.[47] In another prominent case, Shi Tao, a former journalist, was sentenced to 10 years in prison in 2003 on charges of "leaking state secrets" after a message he sent from his Yahoo! e-mail account was intercepted and turned over to the authorities.[48] Huang Qi, an outspoken human rights activist, was detained in July 2008 on similar charges of "illegal possession of state secrets" for posting criticism of Sichuan earthquake relief efforts on his website.[49] In November 2008, Liu Jin, a former university librarian, was sentenced to three years in prison in Shanghai on charges of "using a heretical organization to undermine implementation of the law" after she downloaded information about the Falun Gong from the internet and passed it to others, which her lawyer argues is a common occurrence.[50] According to Reporters Without Borders (RSF), at least 49 cyberdissidents were in jail in China as of July 2008, the largest number of any country in the world.[51] Moreover, prison sentences for online violations tend to be longer in China than elsewhere, often a minimum of three years and as high as ten, while in most other countries punishments range from six months to four years. Though these individuals represent a tiny percentage of the overall user population, the sentencing of prominent individuals within a fairly close-knit activist and blogging community to long prison terms creates a chilling effect and contributes to an atmosphere of fear that extends far beyond the immediately affected group.

While some exist, the options for anonymous online communication are limited, and restrictions have increased in recent years. After significant protests from the internet industry, government attempts to implement real-name registration across all commercial websites have been abandoned for the moment. However, real-name registration has been put into practice among the BBS websites of all the universities.[52] For mobile phones, SIM cards can be purchased anonymously without difficulty, though the transmission of text messages has been more tightly controlled in recent years, and they are frequently intercepted by the Public Security Bureau in cooperation with the MIIT.[53]

Surveillance of internet and mobile-phone communications in China is pervasive and among the most advanced in the world. The country's international gateways form one layer of the monitoring system. Other measures include requirements that users register with ISPs when purchasing internet access at home or at work, which facilitates tracking by the authorities.[54] Customers at cybercafes are required to present identification, and the cybercafes must install software to monitor and filter users' web browsing. In some cities, cybercafes have been required to

---

[46] "Gao Zhisheng, the lawyer "who defies the Communist Party", *AsiaNews,* February 17, 2006,www.asianews.it/view.php?l=en&art=5416 Accessed on 3/23/2009

[47]"China: Dissident writer Chen Daojun sentenced", *English Pen*, November 25, 2008, http://www.englishpen.org/writersinprison/bulletins/chinadissidentwriterchendaojunsentenced/ Accessed on 3/23/2009

[48] "Another cyberdissident imprisoned because of date provided by Yahoo", *Reporter Without Borders*, February 9, 2006,http://www.rsf.org/article.php3?id_article=16402 Accessed on 3/23/2009

[49] "Free Huang Qi", *International Herald Tribune*, February 8, 2009, http://www.iht.com/articles/2009/02/08/opinion/edhuang.php Accessed on 3/23/3009

[50] "China imprison Falun Gong follower, lawyer says", *Associated Press*, November 14, 2008, http://www.iht.com/articles/ap/2008/11/14/asia/AS-China-Falun-Gong.php Accessed on 3/23/2009

[51] *Reporters Without Borders*, http://www.rsf.org/rubrique.php3?id_rubrique=119 Accessed on 3/23/2009

[52] http://www.cnhubei.com/200511/ca936578.htm Accessed on 3/23/2009

[53] "China will monitor, censor sms messages", *Slashdot*, Juky 3, 2004, http://slashdot.org/article.pl?sid=04/07/03/0035224 Accessed on 3/23/2009 and "China cracksdown on sms", *Journalism.co.uk*, February 7, 2004, http://www.journalism.co.uk/2/articles/5970.php Accessed on 3/23/2009

[54] http://news.1488.com/news/legality/2006/7-17/14-34-1-1.shtml Accessed on 3/23/2009 and http://www.adslsh.com/shenqing.asp Accessed on 3/23/2009

install surveillance cameras that transmit images directly to control systems in local branches of the Ministry of Culture. The Ministry of Culture has endeavored to build a national surveillance platform that unites such local systems and is said to be able to filter any objectionable information transmitted from cybercafes.[55] If ISPs and websites are found to showcase "reactionary materials" or fail to promptly comply with the authorities' orders, they are subjected to fines, may have their servers confiscated by internet police,[56] and can have their licenses revoked by the MIIT.[57] In a more informal mechanism of control, some quasi-governmental associations (for example, the Internet Society of China) have been established to encourage domestic websites to implement self-regulation and comply with party orders.

Though they are not experienced by the average user, extralegal intimidation and harassment, including occasional physical violence, have been increasing in recent years as more individuals record, investigate, and publish online information that is deemed undesirable by the government. In January 2008, construction company executive Wei Wenhua was beaten to death in Hubei province by 50 law enforcement officers after he used his mobile phone to film them in a violent clash with demonstrators protesting waste-dumping in their neighborhood. Several of the officers were reportedly detained and later charged over the incident, which marked the first death of a citizen journalist in China.[58] In September 2008, Liu Shaokun, a teacher in Sichuan province, was sentenced to one year of "reeducation through labor" after posting online photos of schools that collapsed in the earthquake; following an international campaign on his behalf, he was released to serve his sentence at home.[59] Individuals known for expressing critical views of the government, such as Hu Jia, his wife Zeng Jinyan, and democracy activist and Charter 08 drafter Liu Xiaobo, have been placed under house arrest or 24-hour police surveillance for months at a time—or for the duration of important domestic and international events—even when they are not formally imprisoned. As with other detainees, individuals arrested for internet-related activities are likely to face severe torture once in custody. This treatment is aimed at forcing them to reveal information or renounce their views or beliefs. Other forms of harassment include visits from police and public security agents, and restrictions on travel, both within and outside the country. In November 2008, Zhou Shuguang (also known as Zola), one of China's best-known bloggers, was prevented from traveling to Hong Kong en route to Germany, where he was set to serve as a judge for an international blogging competition.[60] In addition to persecution from the government, individuals have also been known to suffer harassment from internet mobs, particularly those made up of ultranationalists. Wang Qinyuan, a college student at Duke University, was harassed along with her family in China after she expressed opinions in support of the rights of Tibetans. Her personal information was also posted on the internet, a phenomenon that has been dubbed "human flesh search engine."[61]

---

[55] http://www.netbarcn.net/Html/PolicyDynamic/010619543882 52.html Accessed on 3/23/2009

[56] Personal communication

[57] http://www.zcxybbs.cn/thread-328-1-1.html Accessed on 3/23/2009

[58] "Brutal killing of (citizen journalist) Wei Wenhua underscores the evils of China's "urban management" system", *China Media Project, http://cmp.hku.hk/2008/01/10/814/* Accessed on 3/23/2009

[59] "Mr. Liu Shaokun released to serve his RTL sentence outside of labour camp", *International Federation for Human Rights*, October 16, 2008, http://www.fidh.org/spip.php?article5937 Accessed on 3/23/2009

[60] "Blogger Zhou Shuguang a.k.a. "Zola" barred from leaving China: "potential threat to state security"", *RCConversation*, November 24, 2008, http://rconversation.blogs.com/rconversation/2008/11/blogger-zhou-sh.html Accessed on 3/23/2009

[61] "New freedom, and peril, in online criticism of China", *The Washington Post*, April 17, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/04/16/AR2008041603579.html Accessed on 3/23/2009

Cuba

Status: Not Free

Obstacles to Access: **25** (0–25)
Limits on Content: **32** (0–35)
Violations of User Rights: **33** (0–40)
Total Score: **90** (0–100)

Population: 11.2 million
Internet Users/Penetration 2006: 190 thousand / 2 percent
Internet Users/Penetration 2008: 1.3 million / 11 percent
(Note: includes users with access only to intranet)
Mobile Phone Users/Penetration 2006: 152 thousand
Mobile Phone Users/Penetration 2008: 327 thousand
Freedom of the Press (2008) Score/Status: 94 / Not Free
Digital Opportunity Index (2006) Ranking: 129 out of 181
GNI Per Capita (PPP): Unavailable
Web 2.0 Applications Blocked: Yes
Political Content Systematically Filtered: No
Bloggers/Online Journalists Arrested: Yes

Introduction

Despite the slight loosening of restrictions on the sale of computer and mobile-phone equipment in 2008, Cuba remains one of the world's most repressive environments for the internet and information and communication technologies (ICTs). There is almost no access to internet applications other than e-mail, and surveillance is extensive. Nevertheless, a nascent community of bloggers has emerged on the island, creatively using online and offline means to express opinions and circulate information about Cuban society.

Cuba was connected to the internet for the first time in 1997, and the National Center for Automated Interchange of Information (CENIAI), the country's first internet service provider (ISP), was established that year. However, the executive authorities continue to control the legal and institutional structures that decide who has access to the internet and how much access will be permitted.[1]

Obstacles to Access

Though the government has claimed that all Cubans have access to the internet, according to the ITU, only 1.3 million people – 11.5 percent – had access to the internet in 2008.[2] However, it should be noted that this number is also potentially over inflated as it includes those who had access to the Cuban intranet only, but not to the global internet. A closer estimate is that 240,000 – 2.1 percent – of the population had some level of access to the world wide web in 2008.[3] Restrictions on access have been exacerbated by tight government control over related equipment. The sale of modems was banned in 2001, and the sale of computers and computer accessories to the public was banned in 2002. Exceptions could be authorized by the Ministry of Internal Commerce if the items in question were deemed to be "indispensable." This policy changed in early 2008, when the government of President Raul Castro began allowing Cubans to buy personal computers. Individuals can now legally purchase a computer and connect to an ISP with a government permit. Nonetheless,

1 Ben Corbett, This is Cuba: an outlaw culture survives, Westview Press, 2002, http://books.google.com/books?id=N2P5n3rU7EkC&pg=PA145&lpg=PA145&dq=CENIAI+Internet&source=bl&ots=33reH-Vvh7&sig=UBxsUT16g0Z2BLKa0P1e5NMRFB0, Accessed March 20, 2009.
2 Internet World Stats, http://www.internetworldstats.com/stats10.htm#spanish, Accessed March 20, 2009.
3 Reporters Without Borders, http://www.rsf.org/article.php3?id_article=26096, Accessed March 20, 2009.

high costs put both the internet and mobile phones beyond the reach of most of the population. A simple computer with a monitor averages around 722 convertible pesos (US$780) in retail stores, or at least 550 convertible pesos (US$600) on the black market.[4] By comparison, the average monthly Cuban salary is approximately 16 convertible pesos (US$17).[5] These computers are generally distributed by the state-run Copextel Corporation, which imports communications, computing, and other ICT equipment. An internet connection costs between 6 and 12 convertible pesos (US$9 and US$15) per hour.

According to the International Telecommunication Union (ITU), Cuba had a mobile-phone penetration rate of only 2.9 percent (approximately 327,000 users) as of 2007. However, the government eased restrictions on mobile-phone purchases in March 2008, and reduced the sign-up fee by half, though it still represents three months of wages for the average worker. It is estimated that Cubans signed some 7,400 new contracts for mobile phones in the 10 days following the lifting of the ban, and according to the state-run newspaper *Juventud Rebelde*, an estimated 480,000 cellular lines were in use by year's end.[6] ETECSA, the state-controlled telecommunications company, predicts that there will be 1.4 million new mobile contracts over the next five years.[7] Mobile phones do not include internet connections, but it is possible to send and receive international text messages with certain phones.

The government divides access to web technology between the national intranet and the global internet; most Cubans only have access to the former, which consists of a national e-mail system, a Cuban encyclopedia, a pool of educational materials and open-access journals, Cuban websites, and foreign websites that are supportive of the Cuban government.[8] Cubans can legally access the internet only through government-approved institutions, such as the approximately 600 *Joven Clubs de La Computacion* (Youth Computation Clubs) and points of access run by ETECSA; users are generally required to present identification to use computers at these sites.[9] Many neighborhoods in the main cities of Havana and Santiago advertise "internet" access in ETECSA kiosks, but field research has found that the kiosks often lack computers. Instead they have public phones for local and international calls with prepaid phone cards. The government also claims that all schools have computer laboratories; in practice, however, internet access is usually prohibited for students or limited to e-mail and supervised activities on the national intranet.

Individuals who do access the internet face paralyzingly slow connections, and tests conducted on the island found that just two e-mails could be sent per hour using Yahoo! mail. Multimedia applications were inoperable. This was the case even at universities, where the connections are slightly better than at ETECSA access points.[10] One segment of the population that enjoys approved access to the internet is the professional class of doctors, professors, and government officials. For example, 3,000 e-mail accounts had been issued to medical institutions by 2001, and facilities like hospitals, polyclinics, research institutions, and local doctors' offices are linked via an online network called Infomed.[11] However, even these users are typically restricted to e-mails and sites related to their activities. Beginning in 2007, the government systematically blocked core internet portal sites such as Yahoo!, MSN, and Hotmail. This ban was extended to blog platforms and blog commentary technology during certain periods in 2008. As a result, Cubans

4 "Cubans queue for computers as PC ban lifted, but web still outlawed," *Irish Examiner*, May 5, 2008.
5 "Mobile phone use booms in Cuba following easing of restrictions," Agence France-Presse, April 24, 2008.
6 Cellular News, http://www.cellular-news.com/story/35917.php?s=h, Accessed March 18, 2008.
7 "Mobile phone use booms in Cuba following easing of restrictions," Agence France-Presse, April 24, 2008.
8 ETECSA: Empressa de Telecomunicaciones de Cuba S.A., www.enet.cu, Accessed March 20, 2009.
9 Joven Clubs de La Computacion, http://www.cfg.jovenclub.cu/, Accessed March 20, 2009.
10 ETECSA: Empresa de Telecomunicaciones de Cuba S.A.
11 Infomed, www.sld.cu, Accessed March 20, 2009.

cannot access blogs written by their fellow citizens. Moreover, Voice over Internet Protocol (VoIP) remains blocked in Cuba, with the exception of illegal points of connection in old Havana. Some social-networking platforms such as Facebook are accessible in university cybercafes.

There are only two ISPs, CENIAI Internet and ETECSA, and both are owned by the state. Cubacel, a subsidiary of ETECSA, is the only mobile-phone carrier. In 2000, the Ministry of Information Science and Communication was created to serve as the regulatory authority for the internet, and its Cuban Supervision and Control Agency oversees the development of internet-related technologies.[12] In May 2008, Deputy Minister for Information Science and Communication Boris Moreno said "Cuba is not concerned with the individual connection of its citizens to the internet. We use the internet to defend the Revolution and the principles we believe in and have defended all these years."[13] The government argues that access restrictions are a direct consequence of the U.S. embargo, which prevents Cuba from connecting to underwater cables and forces it to use expensive Chinese and Venezuelan satellites instead.[14] It has been estimated that the cost of laying a fiber-optic cable from Havana to Florida, to allow high-speed connectivity, would cost as little as $500,000.[15] In the meantime, Cuba and Venezuela signed documents in 2006 for the purpose of building and operating a fiber-optic cable linking Cuba and Venezuela (as well as Jamaica, Haiti, and Trinidad and Tobago) and amplifying Cuba's internet connections by 2010.[16] It remains unclear whether the Cuban government will truly allow widespread access once the infrastructural impediments are removed.

Limits on Content

Rather than engaging in the technically sophisticated blocking and filtering used by other repressive regimes such as China and Tunisia, Cuban authorities rely heavily on lack of technology and prohibitive costs to limit users' access to information. The websites of foreign news outlets—including the British Broadcasting Corporation (BBC), *Le Monde*, and the *Nuevo Herald* (a Miami-based Spanish-language daily)—and human rights groups like Amnesty International and Human Rights Watch remain largely accessible, though slow connection speeds impede access to the content on these sites.[17] Sites and writings that are considered anti-Cuban or counterrevolutionary are restricted. These include many of the Cuban dissident sites based in the United States and abroad, and any documents containing criticism of the current system or mentioning dissidents, supply shortages, and other politically sensitive issues.[18] Blogs written by Cubans residing in Cuba are also inaccessible. For example, sites such as cubanet.org, payolibre.com, bitacoracubana.com, cubadebate.com, and prolibertadprensa.blogspot.com cannot be accessed at the youth computer centers. It is a crime to contribute to international media that are not supportive of the government, a fact that has led to widespread self-censorship. Cuban blogs typically feature implicit or explicit elements of self-censorship and anonymity. Many of those working closely with ICT's are journalists who have been barred from official employment, and the prohibitive costs surrounding the

[12] Ministry of Information Science and Communication, http://www.mic.gov.cu/, Accessed March 20, 2009.
[13] "In Raul Castro's reforms in Cuba, internet remains restricted," Agence-France-Presse, May 17, 2008, http://afp.google.com/article/ALeqM5gbs2d7rh33vYKZ6hp3xAwhA4BXvQ, Accessed March 20, 2009.
[14] For instance, Government sources cite the cost of 4 million US$/yr to connect to the Internet through these satellites. From this, local sources affirm that 850K US$/yr are just to connect a local association of artists and writers.
[15] "Cuba to get high-speed Internet in 2010," Techweb, July 17, 2008
[16] Ibid.
[17] "Access impeded to Internet platform hosting popular blogs, other websites," March 31, 2008, http://www.ifex.org/en/content/view/full/92118/,Accessed March 20, 2009.
[18] ONI report on Cuba, http://opennet.net/research/profiles/cuba, Accessed March 12, 2009.

technology represent a major obstacle for them. The majority of their work is done offline by hand, typewriter, or computer, then uploaded and published once or twice a week using a paid internet access card. For those contributing to international outlets, content can be dictated via costly international phone calls.

Despite all of these barriers, Cubans still connect to the internet through both legal and illegal points of access. Some are able to break through the infrastructural blockages by building their own antennas, using illegal dial-up connections, and developing blogs on foreign platforms. The underground economy of internet access also includes account sharing, in which authorized users sell access to those without an official account for one or two convertible pesos per hour. Some foreign embassies allow Cubans to use their facilities, but a number of people who have visited embassies for this purpose have reported police harassment. To date there have been no reported cases of Cuban activists using mobile phones or SMS (text messaging) to organize events or disseminate political information. However, there is a thriving improvisational system of "sneakernets," in which USB keys, CDs, and DVDs are used to distribute material (articles, satirical cartoons, video clips) that has been downloaded from the internet.

The lack of a proper internet connection remains Cuban bloggers' biggest challenge, according to Roger Trabas, cofounder of the Bloggers Cuba website. In September 2008, Trabas organized the first meeting—dubbed Blogging on Our Own—designed to bring together the island's bloggers and those involved in online journalism.[19] There is no exact count of blogs produced in Cuba, but the Cuban Journalists' Union (UPEC) has reported a current total of 174. Examples include Yoani Sanchez's famous blog *Generación Y*, which draws 26 percent of its readers from within Cuba, as well as sites like *Retazos*, *Nueva Prensa*, *PayoLibre.com*, *Cubaencuentro.com*, and *Convivencia*. Regional radio stations and magazines are also creating online versions, though these outlets are state-run and do not accept contributions from independent journalists. However, in a recent development, some of these sites have installed commentary tools that allow readers to provide feedback and foster discussion.

Cubans succeeded in mobilizing via the intranet in January 2007, following the appearance of Luis Pavon Tamayo on a television program honoring people who have made significant contributions to Cuban culture. Cuban artists and intellectuals spontaneously started an e-mail discussion to protest his appearance. Tamayo had formerly headed the National Culture Council and was widely viewed as responsible for a multiyear crackdown on cultural expression during the 1970s. The period, known as the Grey Five, saw Cuban artists and intellectuals censored, sent to labor camps, or driven into exile. The e-mail protest quickly drew the attention of the government, and Culture Minister Abel Prieto met with 20 of those involved to discuss their concerns.[20] Prieto initially refused to apologize for Tamayo's appearance, but in the face of a growing online movement he reconsidered and issued an apology. He said the appearance—as well as the subsequent appearances of two other leading figures in the 1970s crackdown, Armando Quesada and Jorge Serguera—had been an "error," and explained that "today the leadership of this country regards that period—which was fortunately brief—with great disapproval."[21]

---

19 "Cuba: More Bloggers are Firing Off Thoughts From the Island," Inter Press Service, October 6, 2008.

20 "Cuban writers angered by resurfacing of censor," January 16, 2007, http://www.caribbeannetnews.com/cgi-script/csArticles/articles/000051/005155.htm , Accessed March 20, 2009.

21 "Artists' congress marks more changes in Cuba," April 5, 2008, http://www2.canada.com/vancouversun/news/story.html?id=c97b6387-8824-4198-8910-9cc9b06ac8c6, Accessed March 20, 2009. and Arturo Gracía Hernàndez, "Interview with Abel Prieto, Cuban Minister of Culture," www.embacu.cubaminrex.cu/Portals/7/Interview.doc , Accessed March 20, 2009.

Violations of Users' Rights

The legal structure in Cuba is not favorable to internet freedom. There is no clear constitutional guarantee of internet freedom, and the constitution explicitly subordinates freedom of speech to the objectives of socialist society.[22] Freedom of cultural expression is guaranteed only if the expression is not contrary to the Revolution.[23] The penal code and Law 88 set penalties ranging from a few months to 20 years in prison for any activities that are considered a "potential risk," "disturbing the peace," a "precriminal danger to society," "counterrevolutionary," or "against the national independence or economy."[24]

Cuba is one of the few countries to have issued laws and regulations explicitly restricting and outlawing certain online activities. In 1996, the government passed Decree-Law 209, known as Access from the Republic of Cuba to the Global Computer Network, which states that the internet cannot be used "in violation of Cuban society's moral principles or the country's laws," and that e-mail messages must not "jeopardize national security."[25] In 2007, Resolution 127 on network security banned the spreading of information via public data-transmission networks that is against the social interest, norms of good behavior, the integrity of people, or national security. The decree requires access providers to install controls that will enable them to detect and prevent the proscribed activities, and to report them to the relevant authorities.

From a regulatory perspective, Resolution 56/1999 provides that all materials intended for publication or dissemination on the internet must first be approved by the National Registry of Serial Publications. Moreover, Resolution 92/2003 prohibits e-mail and other ICT service providers from granting access to individuals who are not approved by the government, and requires that they enable only domestic chat services, not international ones. Entities that violate these regulations can have their authorization to provide access suspended or revoked.

Despite constitutional provisions that protect various forms of communication, and portions of the penal code that set penalties for the violation of the secrecy of communications, the privacy of users is frequently violated in practice. Tools of content surveillance and control are pervasive, from public access points and universities to government offices. Delivery of e-mail messages is consistently delayed, and it is not unusual for a message to arrive without its attachments. The phenomenon is known to occur in hotel cybercafes used by both tourists and locals.

The new administration of Raul Castro has continued its predecessor's repressive practices with respect to independent journalism, indirectly affecting the blogging community as well. These practices include the imposition of fines, searches, and the confiscation of money and equipment. There have been a few cases in which online journalists were arrested and punished for their work, most notably the imprisonment of two correspondents of CubaNet. One, Oscar Sanchez Madan, was sentenced to four years in prison in April 2007 for "precriminal social danger," and the other was sentenced to seven years in November 2005 for "subversive propaganda."[26] Still, bloggers have not been subject to anything akin to the Black Spring of 2003, in which 27 journalists were arrested on grounds that they were "agents of the American enemy."[27]

---

[22] Article 53, available at http://www.cubanet.org/ref/dis/const_92_e.htm, Accessed March 20, 2009.
[23] Article 39, d), available at http://www.cubanet.org/ref/dis/const_92_e.htm, Accessed March 20, 2009.
[24] See – Protection of Cuba's National Independency and economy. http://cpj.org/reports/2008/03/laws.php
[25] Cuba – Telecoms Market Overview & Statistics 2008.
[26] Freedom of the Press, Cuba 2008, http://www.freedomhouse.org/template.cfm?page=251&year=2008 , Accessed March 12, 2009.
[27] Reporters Without Borders, March 16, 2006, http://www.rsf.org/article.php3?id_article=16771 , Accessed March 20, 2009.

Prominent bloggers do face a wide range of other forms of harassment, intimidation, and restrictions on their rights. Yoani Sanchez and her husband Reynaldo Escobar (a fellow blogger) were summoned for questioning in December 2008, reprimanded, and informed that their right to travel had been restricted, meaning they would be unable to attend a two-day blogging workshop in the western part of the island.[28] Other individuals planning to attend the event were also summoned for questioning and pressured to cancel;[29] as a result, the meeting of 20 bloggers was reportedly held online to avoid the risk of arrest.[30] In May 2008, the government refused to issue Sanchez a travel visa that would have allowed her to receive the Ortega y Gasset prize for digital journalism in Spain.[31]

[28] "Cuba v. the Bloggers," PoliBlog, December 6, 2008.

[29] Global Voices Online, Cuba Government Officials Tell Bloggers to Cancel Planned Meeting, December 6, 2008, http://advocacy.globalvoicesonline.org/2008/12/06/cuba-government-officials-tell-bloggers-to-cancel-planned-meeting/ , Accessed March 20, 2009.

[30] Mother Jones, http://www.motherjones.com/politics/2008/12/cubas-blogger-crackdown, Accessed March 20, 2009.

[31] "Cuba refuses to give blogger visa to collect prize," Agence France Press, May 6, 2008.

Egypt

Status: Partly Free

Obstacles to Access: **8** (0–25)
Limits on Content: **11** (0–35)
Violations of User Rights: **26** (0–40)
Total Score: **45** (0–100)

Population: 76.8 million
Internet Users/Penetration 2006: 5.1 million / 7 percent
Internet Users/Penetration 2008: 10.7 million / 14 percent
Mobile Phone Users/Penetration 2006: 18 million
Mobile Phone Users/Penetration 2008: 31 million
Freedom of the Press (2008) Score/Status: 59 / Partly Free
Digital Opportunity Index (2006) Ranking: 91 out of 181
GNI Per Capita (PPP): $5,400
Web 2.0 Applications Blocked: No
Political Content Systematically Filtered: No
Bloggers/Online Journalists Arrested: Yes

Introduction

While the Egyptian government has aggressively and successfully sought to expand access to the internet as an engine of economic growth, its security services and allied individuals have increasingly attempted to curtail the use of new technologies for disseminating and receiving sensitive political information. This is usually through such "low-tech" methods as intimidation, legal procedures, detentions, and real-world surveillance of online activists.

Egypt first introduced access to the internet in October 1993 through the Egyptian Universities Network and the Egyptian cabinet's Information and Decision Support Center (IDSC). The prime minister, the minister of communications and information technology, and the heads of the country's leading internet service providers (ISPs) are all graduates of the IDSC, a fact that may explain the civilian government's internet-friendly policy. The public first gained access in 1996, but the technology did not really take off until 2002, when the government introduced a "Free Internet" program, whereby anyone with a telephone line and a computer could access the internet for the price of a local call ($0.15 an hour). Offline repression of online activists is sporadic and keyed to sensitive political events.

Obstacles to Access

Access to digital communications has grown exponentially since it was first made available to the public in 1996, but widespread poverty and poor infrastructure, particularly in rural areas, remain barriers to access. According to government statistics, 0.58 percent of the population used the internet regularly in 1999. By 2008, the figure had grown to 14 percent and 10.7 million users.[1] Broadband internet, while widely available, remains prohibitively expensive for most of Egypt's population, 40 percent of which lives on $2 or less a day.[2] In 2008, just over 1 percent of the population had a broadband connection at home, but internet cafes offering such connections are common, even in urban slums and small villages. In December 2008, an average of 200,000 people a week used these cafes. Also in 2008, 31 million people had a mobile telephone.[3] Later generation

1 International Telecommunications Union via "Internet world stats": http://www.itu.int/ITU-D/icteye/Default.aspx, Accessed on March 10, 2009
2 World Bank and Ministry of Economic Development poverty assessment update, 2007
3 ITU, http://www.itu.int/ITU-D/icteye/Default.aspx, Accessed on March 10, 2009

mobile phones, such as Apple's iPhone, are available in the country, but without the Global Positioning System (GPS) feature, as the authorities have banned the technology, claiming it would enable terrorists to target military installations.[4] The video-sharing site YouTube, the social-networking site Facebook, and international blog-hosting services are freely available.

More than 200 ISPs serve Egypt's population of roughly 80 million people, but Link.net and TE-Data are by far the largest.[5] Most ISPs lease bandwidth from these two companies, both of which are run by men with close connections to the government. Three mobile-phone operators—Vodafone, Mobinil, and most recently the Dubai-based Etisalat—serve Egyptian subscribers. All three offer broadband internet connections via USB modems. Mobile-phone services and ISPs are regulated by the National Telecommunication Regulatory Authority (NTRA) pursuant to the 2003 Telecommunication Law. The NTRA's board is currently chaired by Minister of Internet and Communications Technologies Tariq Kamel, but it also includes representatives of the president, the ruling party, the interior and defense ministries, and the country's domestic intelligence service, State Security Investigations.[6] There have been no reported incidents of ISPs being denied registration permits.

Limits on Content

The Egyptian government does not engage in widespread censorship of the internet.[7] Court cases against traditional journalists and "friendly" phone calls from military or security officers to both journalists and activists have established such topics as the military, the president's health, Muslim-Christian tensions, and torture as sensitive topics that must be handled with particular care, if at all. However, online writers routinely disregard most of these "red lines," often with impunity. Some ISPs offer subscribers "family internet" packages that block access to pornography and sites advocating violence, in exchange for a small premium.

In the past four years, Egypt has witnessed the birth of a lively and diverse "blogosphere." Many bloggers have become media celebrities and have won international awards for their work. This in turn may have helped spur interest in blogging among young Egyptians. As the number of blogs has increased, so has the diversity of opinion and content. Lesbian and gay Egyptians compete for space and attention on the internet with activists from the conservative Muslim Brotherhood. Opposition and human rights activists have found innovative ways to use blogs and social-networking sites such as Facebook and Jaiku to call attention to causes and organize protests. In some cases, they have succeeded in doing what traditional activists rarely have. In 2007, a Cairo court sentenced two police officers to three years in prison for beating and raping a microbus driver based on video evidence first obtained by Egyptian blogger Wael Abbas, who posted the video on YouTube.[8] Egyptian bloggers have also played a crucial role in focusing the government's and the media's attention on the problem of sexual harassment of women on the streets of Cairo. The

---

[4] *The Telegraph*, http://www.telegraph.co.uk/scienceandtechnology/technology/3687651/Apple-removes-GPS-from-iPhone-sold-in-Egypt-over-security-fears.html , Accessed March 20, 2009.
[5] Ministry of Communications and Information Technology Web site, "Telecom Reform Milestones," http://www.mcit.gov.eg/tele_Mileston.aspx, Accessed March 10, 2009.
[6] National Telecommunication Regulatory Agency Web site, http://www.tra.gov.eg/english/DPages_DPagesDetails.asp?ID=175&Menu=5, Accessed March 10, 2009.
[7] Open Net Initiative, Egypt Country Profile, http://opennet.net/research/profiles/egypt, Accessed March 10, 2009.
[8] "Egypt: Police Officers Get Three Years for Beating, Raping Detainee," Human Rights Watch, November 6, 2007, http://www.hrw.org/en/news/2007/11/06/egypt-police-officers-get-three-years-beating-raping-detainee?print, Accessed March 10, 2009.

publicity generated by their reporting has given rise to dozens of governmental and civil-society campaigns seeking an end to the problem, and the police have begun to take action.[9]

Violations of Users' Rights

No laws specifically grant the government the power to censor the internet, and authorities have resisted calls to censor websites.[10] Egypt's constitution upholds freedom of speech, and the 2003 Law on Telecommunications as well as guaranteeing a citizens' right to privacy, also requires a judicial warrant for surveillance.[11] However, articles of the penal code and the Emergency Law, which has been in effect without interruption since 1981, give security agencies broad authority to monitor and censor all communications.[12] Amendments to the Press Law passed in 2006 preserved provisions that criminalize "spreading false news" and criticizing the head of state of Egypt or another country,[13] and courts have ruled that these restrictions apply to online writings.[14] Constitutional amendments passed in 2007 paved the way for future counterterrorism legislation that could uphold Emergency Law provisions allowing for widespread surveillance.[15] Nevertheless, in December 2007 an administrative court judge issued a decision rejecting a request by a fellow member of the judiciary to ban 51 Egyptian websites, including those of several human rights organizations. In his decision, the judge emphasized the importance of respecting freedom of expression, including on the internet.[16]

It is difficult to gauge the extent to which Egyptian security services monitor internet and mobile-phone communications, but the surveillance is believed to be far-reaching. Among the evidence pointing to this conclusion are the recent detention of two activists for using Facebook to organize strikes (see below), and the anecdotal reports that police often appear in advance at the sites of protests that were planned by text messages and e-mail. Those speaking on mobile phones to known activists and journalists within Egypt report that they frequently hear a suspicious echo or strange clicks and beeps. The legal environment allows for such surveillance, and indeed the security services have sought to perpetuate the impression that their monitoring is pervasive. At least one security officer has boasted in the press that the internet is monitored in real time.[17] In addition, security services use legal and extralegal means to collect internet and mobile-phone users' records from ISPs, internet cafes, and mobile-phone companies in the course of their investigations.

To date, only one person has been sentenced to prison in Egypt for his online activities, but security services have used detentions and harassment, and in some cases torture, to intimidate

9 "550 Schoolgirls harassed in one day," Al-Arabiya, November 20, 2008, http://www.alarabiya.net/articles/2008/11/20/60477.html, Accessed March 10, 2009.

10 Report of the State Commissioner Committee, June 2007, in response to Judge Abd al-Fatah Murad's lawsuit demanding the state censor 51 web sites of human rights organizations and blogs on national security grounds, on file with the author. The committee rejected the law suit after government lawyers explained why the government did not want to begin censoring the Internet.

11 Law 10 of 2003, article 65.

12 Law 162 of 1958, renewed in 1981.

13 Law 147 of 2006.

14 *International Herald Tribune*, http://www.iht.com/articles/2007/02/26/opinion/edblog.php, Accessed March 20, 2009.

15 "Egypt: Proposed constitutional amendments greatest erosion of human rights in 26 years," Amnesty International, March 18, 2007, http://www.amnesty.org/en/library/asset/MDE12/008/2007/en/dom-MDE120082007en.html, Accessed March 10, 2009.

16 "Court rejects request to ban 51 websites," Arabic Network for Human Rights Information, http://www.ifex.org/en/content/view/full/89371, Accessed March 25, 2009

17 Egypt Internet Country Profile, Reporters sans frontieres, http://www.rsf.org/article.php3?id_article=10732, Accessed March 10, 2009.

online writers. On February 22, 2007, Abd al-Karim Nabil Suleiman (widely known as Karim Amer), then a 22-year-old student of religious law at Al-Azhar University, became Egypt's first blogger to be sentenced to prison for his online writings. A court in Alexandria handed Suleiman a four-year prison term on charges of "insulting Islam" and "insulting the president."[18] On March 10, 2007, blogger Mohammad al-Sharqawi, who had previously been tortured for participating in a street protest, returned home to find that his laptop, which he said contained an unreleased video depicting police abuse, had been stolen, though cash and other valuable items were not taken.[19] On April 14, 2007, security officers arrested Muslim Brotherhood–affiliated blogger and journalist Abd al-Monim Mahmud. He had recently blogged about his experience of torture in 2003. He was held for 47 days on charges of belonging to a banned organization before being released without trial.[20] Security forces arrested Isra Abd al-Fattah for using Facebook to call for a general strike on April 6, 2008. She was held for two weeks, despite a prosecutor's decision to dismiss charges of "inciting unrest," before her eventual release on April 23. And in May, state security officers detained and beat Ahmed Maher, a 27-year-old engineer who had also used Facebook to call for a general strike to mark President Hosni Mubarak's 80th birthday three days prior. The officers released Maher without charge the next night, but warned him that he would be beaten more severely the next time he was detained.[21] Others have received less-publicized threats and low-level harassment. This focus on legal repercussions and extra-judicial intimidation for online activity is the primary method of state control of an otherwise relatively open medium, and although recent, appears set to increase.

[18] "Internet Enemies: Egypt," Reporters sans frontieres, 2008, http://www.rsf.org/article.php3?id_article=26150&Valider=OK, Accessed March 10, 2009.
[19] Interview with the author, March 12, 2007.
[20] Interview with the author, June 15, 2007.
[21] Interview with the author, May 8, 2008.

Estonia

Status: Free

Obstacles to Access: **2** (0–25)
Limits on Content: **2** (0–35)
Violations of User Rights: **6** (0–40)
Total Score: **45** (0–100)

Population: 1.3 million
Internet Users/Penetration 2006: 690 thousand / 52 percent
Internet Users/Penetration 2008: 852 thousand / 64 percent
Mobile Phone Users/Penetration 2006: 1.7 million
Mobile Phone Users/Penetration 2008: 1.9 million
Freedom of the Press (2008) Score/Status: 16 / Free
Digital Opportunity Index (2006) Ranking: 24 out of 181
GNI Per Capita (PPP): $19,800
Web 2.0 Applications Blocked: No
Political Content Systematically Filtered: No
Bloggers/Online Journalists Arrested: No

Introduction

Estonia ranks among the most wired and technologically advanced countries in the world. The first internet connections in the country were introduced in 1992 in Tallinn and Tartu academic facilities. According to Estonia's president, the country's status as an "e-country" is due in large part to the disastrous condition of the country's infrastructure in 1991 following nearly 50 years of Soviet control.[1] In an effort to integrate Estonia into the global economy, the government initiated a program entitled Tiger Leap that aimed to computerize and connect all Estonian schools with the internet by 2000. This program helped to build competence and awareness about information and communication technologies (ICTs). Today, with such a high level of computer literacy and connectivity, focus has shifted from basic concerns such as access, quality, and cost of internet services to discussions about security, anonymity, the protection of private information, and citizens' rights on the internet. These issues are closely tied to the most serious threat to internet freedom in Estonia, namely, the cyber attacks against various Estonian communication infrastructures in late April and early May 2007.

Obstacles to Access

The number of internet and mobile phone users in Estonia has grown rapidly in the past 15 years. The internet is regularly accessed by two-thirds of Estonian's population, or approximately 852,000 people;[2] 58 percent of households have internet access, and virtually all of them (90 percent) have a broadband connection.[3] There are also 1.9 million mobile phone subscribers—600,000 more than Estonia's population. The first public WiFi covered area was launched in 2001, and since then the country has developed a system of 2.5G and 3G mobile data networks that enable widespread wireless broadband access. In August 2008, the government announced that by 2009 the country would have 2,000 free certified WiFi covered areas meant for public use, including cafés, hotels,

[1] "Estonia Became Internet Savvy "Thanks" to Occupation," Baltic News Service, April 15, 2008.
[2] ITU, http://www.itu.int/ITU-D/icteye/Default.aspx.
[3] http://www.stat.ee/18959, accessed December 2008.

motels, and even gas stations.[4] In addition, the countrywide wireless internet service based on CDMA technology—which propagates very well due to the use of a low radio frequency—has been deployed and priced to compete with fixed broadband access. Municipalities in rural areas have been subsidizing local wireless internet deployment efforts, and the country's regulatory framework enables local start-ups to provide service with low barriers to entry. Estonians use the internet for a large variety of activities, including search engines (85 percent of users), e-mail (83 percent of users), local online media, news portals, social networking sites, instant messaging, and internet voice communication solutions.[5] Additionally, 83 percent of the population uses the internet for online banking—the second highest percentage in the European Union.[6] Estonian Public Broadcasting delivers all radio channels in real time over the internet, including audio archives of its radio and television programs, at no charge to users. Emphasis on communication and social media services are an increasing trend. YouTube, Facebook, LinkedIn, Orkut and many other global streaming media and social networking sites are widely available and used.

Data communication has not been the subject of telecommunications service monopoly. The Estonian Electronic Communications Act was created to help develop and promote a free market and fair competition in electronic communications services.[7] Today there are over 200 operators that provide a variety of data communication services in Estonia. In 2008, there were eight mobile phone companies, including Elisa, Tele2, and EMT, and numerous major internet-service providers (ISPs), including EENET and Eunet. ISPs and other communications providers are required to register with the Estonian Technical Surveillance Authority (ETSA), a branch of the Ministry of Economic Affairs and Communications, although there is no registration fee.[8]

Limits on Content

Limits on internet content and communication in Estonia are among the lowest in the world. Nevertheless, due in part to Estonia's thorough privacy laws, there are some instances of content removal. Most of these cases are related to civil court orders concerning cases where inappropriate comments or comments unrelated to the posted article were made. This practice also applies to online comments in forums or on web pages where no registration is needed, although IP addresses can be monitored. Generally, users are informed as to the media portals' privacy policy and regulations for commenting and are expected to follow the instructions. In 2008, the debate over self-censoring or pre-publication censorship took center stage in a court case where the victim of unflattering and largely anonymous comments to a news story filed suit claiming that web portals must be responsible for comments made by readers and must edit them before they become public.[9] Web portals say that this is impossible, since they do not have the capacity to monitor and edit all comments made on their sites. The Estonian courts have ruled in favor of the plaintiff, thereby

[4] "Estonia to have 2,000 public WiFi by 2009," Estonian Review, http://brilliantfixer.wordpress.com/2008/08/08/estonia-to-have-2000-public-wifi-areas-by-2009/, accessed March 25, 2009.
[5] http://www.nlib.ee/html/yritus/infofrm3/ipf_pille_runnel.ppt , accessed February 2009.
[6] "Estonians tend to avoid e-shopping – survey," Baltic News Service, February 8, 2008.
[7] Ministry of Economic Affairs and Communications, http://www.mkm.ee/index.php?id=9576 , accessed March 26, 2009.
[8] Estonian Technical Surveillance Authority, Commencement of Provision of Communications Service, http://www.tji.ee/?id=13110, accessed March 26, 2009.
[9] "Big businessman goes to war against web portals," Baltic Business News, March 18, 2008, http://www.balticbusinessnews.com/Default2.aspx?ArticleID=48694078-50cc-4fe1-b3e4-6e10bc6a5ec1.

making web portals responsible for all comments posted, but the ruling is being appealed.[10]

There are over 40,000 active Estonian language blogs on the internet, including an increasing number of group, project, and corporate blogs. The vibrancy of the blogosphere and its activities are frequently covered by traditional media, particularly when blog discussions surround civic activity. The fact that so many Estonians are both computer literate and connected to the internet has created a unique opportunity for the Estonian government. In addition to hosting virtual trade fairs and an online embassy, the Estonian president's office has its own YouTube Channel, complete with messages released exclusively on YouTube.[11] Estonia has the largest functioning public key infrastructure in Europe, based on the use of electronic certificates maintained on the national ID card.[12] More than 80 percent of the population possesses the ID card that enables both electronic authentication and digital signing. Relevant legislation is in place, giving the digital signature equal power with the handwritten one and imposing a responsibility on public authorities to accept digitally signed documents. Estonian ID cards have been used to facilitate electronic voting during parliamentary elections in 2007, and they will be used again in 2009 municipal and European Parliament elections.[13] In 2008, over 86 percent of citizens filed their taxes over the internet, making the online services offered by the tax department the most popular public e-service.

In April 2007, blogs and SMS messaging played an important role in the protests over the removal of a Soviet war monument. While it was known that the Estonian government would remove the monument, no official announcement had been made. When the police cordoned off the area and covered the monument, word quickly spread via mobile phone, SMS, and the internet, and within a few hours the crowd had grown to several thousand.[14] Two days of rioting followed, mostly by ethnic Russians. However, as the physical violence receded, an unprecedented wave of cyber attacks against the Estonian government began. These "dedicated denial of service" (DDoS) attacks affected all of the government's websites, Estonia's largest bank, and several sites of daily newspapers. Because of Estonia's level of connectivity, even simple transactions like reading e-mail, online banking, and paying for a parking space were impossible. Officials were finally forced to block access to Estonian sites from IP addresses outside of Estonia in an effort to stop the attacks.[15] Throughout the three-week period of unrest, internet appeals and SMS messages continued to call for protests against the Estonian government.[16]

Violations of Users' Rights

Freedom of speech and freedom of expression are strongly protected by Estonia's constitution and by its membership in the European Union (EU). Anonymity is allowed, and discussions on anonymity and the respectful use of the internet have been widespread. Internet access at public access points can be obtained without prior registration. In 1996, Estonia enacted the Personal Data Protection Act (PDPA) which protects an individual's personal data from collection and dissemination for public use. Any data that is considered sensitive—political opinions, religious or

[10] "Delfi plans to appeal against the ruling favoring Vjacheslav Leedo," Baltic News, June 30, 2008, http://www.balticbusinessnews.com/Default2.aspx?ArticleID=96dfdecf-baa5-4c68-b112-1fa3a8bf257f.
[11] "Estonia launches embassy in virtual world Second Life," Agence France Presse, December 4, 2007, and http://shaan.typepad.com/shaanou/2008/12/estonian-president-launches-youtube-video-blog.html.
[12] http://id.ee/?lang=en.
[13] http://www.vvk.ee/engindex.html.
[14] Global Voices Online, "A Russia Rebellion," http://globalvoicesonline.org/2007/04/27/estonia-a-russian-rebellion/, accessed March 24, 2009.
[15] "Estonia hit by Moscow cyber war," BBC, May 17, 2007, http://news.bbc.co.uk/2/hi/europe/6665145.stm.
[16] "Estonia launches probe into Internet call for armed uprising," Agence France Presse, May 3, 2007.

philosophical beliefs, ethnic or racial origin, sexual behavior, health, criminal convictions, etc.—cannot be processed without the consent of the individual. The Data Protection Inspectorate (DPI) is the supervisory authority for the PDPA with an objective of "state supervision of the processing of personal data, management of databases and access to public information."[17] However, as a member state of the European Union, Estonia is under pressure to implement the EU Data Retention Directive that requires ISPs and other telecommunications providers to retain customer data for a period of no less than six months and no longer than two years. The EU adopted the Directive in March 2006. However, Estonia chose to postpone the implementation of the Directive for 36 months.[18] At the time of this report, the postponement was still in place.

There have been no physical attacks against bloggers or online journalists in Estonia, but online discussions are sometimes inflammatory. Following instances of cyber bullying, sexual harassment, and misuse of social media, discussions and public awareness campaigns were launched to raise parental involvement and increase child protection on the internet. Awareness of the importance of the security of ICTs both in private and business use has been raised significantly after cyber attacks took place against Estonia in May 2007. Recently, the Cooperative Cyber Defence Centre of NATO was established in Estonia to improve cyber defense interoperability and to provide cyber defense support for all NATO members.[19] Tartu University and Tallinn University of Technology have also announced that they are launching the world's first Master's program in cyber defense.[20]

[17] EPIC Human Rights Report, http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Republic-8.html, accessed March 24, 2009.
[18] DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, Official Journal of the European Union, http://eur-lex.europa.eu/LexUriServ/site/en/oj/2006/l_105/l_10520060413en00540063.pdf, March 24, 2009.
[19] NATO Transformation Network, http://transnet.act.nato.int/WISE/TNCC/CentresofE/CCD.
[20] "Estonian universities to launch Master's programmes in cyber defence," Estonian Review, October 10, 2008.

Georgia

Status: Partly Free

Obstacles to Access: **13** (0–25)
Limits on Content: **15** (0–35)
Violations of User Rights: **12** (0–40)
Total Score: **40** (0–100)

Population: 4.3 million
Internet Users/Penetration 2006: 332 thousand / 8 percent
Internet Users/Penetration 2008: 357 thousand / 9 percent
Mobile Phone Users/Penetration 2006: 1.7 million
Mobile Phone Users/Penetration 2008: 2.6 million
Freedom of the Press (2008) Score/Status: 60 / Partly Free
Digital Opportunity Index (2006) Ranking: 88 out of 181
GNI Per Capita (PPP): $4800
Web 2.0 applications blocked: Yes
Political Content Systematically Filtered: No
Bloggers/Online Journalists Arrested: No

Introduction

Recent years have seen an increase in internet use and mobile-phone penetration in Georgia, though the impact of the new technology in the political sphere remains limited. The government generally does not restrict user access to content, though two significant events during the coverage period of this report influenced the development of the internet in Georgia: the nine-day state of emergency in November 2007 and the conflict with Russia in August 2008.

The internet was introduced at the end of 1990s and experienced a boom after new services like DSL and ADSL became available at the beginning of 2004. Online news media are developing slowly, but more and more journals and newspapers are acquiring domain names and launching websites. The main reason for this slow development is a lack of knowledge about technology and web tools, as well as a poor understanding of how powerful a platform the internet can be. The most developed parts of the Georgian internet are forums, followed by blogs, social-networking sites, and various web 2.0 sites. Restrictions on content and access are neither definitively set nor effectively enforced by law, as evidenced by the huge variety of sites containing illegal material.

Obstacles to Access

The number of internet and mobile-phone users is growing, but high prices for service and a lack of land-line telephone infrastructure remain obstacles to access, particularly for those in rural areas or with low income. The International Telecommunication Union (ITU) estimates that as of 2008 there were approximately 357,000 internet users, for a penetration rate of 8.9 percent.[1] However, additional sources suggest that there was a significant increase in internet use during 2008, so that at year's end the number of users stood at just over 900,000, for a penetration rate of 14.8 percent.[2] Internet usage in the capital, Tbilisi, and in the large city of Batumi is approximately 35 percent, while in other cities the average is around 15 percent.[3] Mobile-phone penetration is more thorough, with a total of 2.6 million users out of a population of 4.3 million.[4] Mobile phones outnumber land lines, and reception is available throughout the country, including in rural areas. However, the use of

[1] International Telecommunications Union, http://www.itu.int/ITU-D/icteye/Default.aspx
[2] http://www.statistics.ge and http://www.top.ge, accessed December 2008 (calculations are the author's)
[3] http://act.ge/index.php?lang_id=ENG&sec_id=296&info_id=369, accessed December 2008
[4] ITU, http://www.itu.int/ITU-D/icteye/Default.aspx

mobile phones to connect to the internet, while growing, is limited by high costs. In January 2007 there were only 5,500 mobile internet users registered, all of them using one service provider, but by end of October 2008 there were 56,500 users and two providers.

Language barriers do not seem to restrict residents' ability to access the internet. While websites do not yet support minority languages, they are widely available in both Georgian and English. The main obstacle to internet access is the lack of modern infrastructure in rural areas, where phone lines and other communications systems are in need of vital maintenance. Economic barriers serve as an additional obstacle, as internet costs are high in relation to the average income. Fixed-line internet providers are reducing fees, but mobile internet providers are not yet changing their pricing policies.

Cybercafes provide internet access for reasonable fees, but they are located mainly in large cities and there are too few to meet the needs of the population. Most cafes have between three and ten computers, and users often have to wait as long as an hour for access. Many restaurants, cafes, bars, cinemas, and other gathering places provide wi-fi access, but not everyone has a laptop or mobile device to take advantage of this type of connection. Mobile-phone companies do not provide automatic internet service to subscribers; users are required to pay an additional fee to subscribe for internet service.

While the authorities do not regularly block access to specific websites, there have been a few cases in which they interfered with internet access on a large scale. In August 2008, the government blocked access to all Russian addresses (those using the .ru country code) in an effort to prevent users from receiving "unofficial" information about that month's conflict. [5] The move was also a response to attacks launched by Russian hackers against Georgian government websites. In addition to limiting access to certain content, the government's action affected Georgian users' ability to access advanced applications based in Russia. Sites such as Livejournal (a popular Russian-owned blogging service), odnoklassniki.ru (the leading social-networking site in Georgia), mail.ru (an e-mail, photo, and blog-hosting service), and yandex.ru (a search engine, e-mail, site-rating, and counter service) were all made unavailable. The filtering was eased within days, and Georgian users were subsequently able to access e-mail services and social-networking sites. The YouTube video-sharing site, the social-networking site Facebook, and international blog-hosting services are freely available.

A separate 2008 dispute, this time between private actors, also affected Georgians' ability to access the internet during the year. It erupted when Georgian Telecom, which owns about 80 percent of all telephone lines in Tbilisi, accused Caucasus Online of not paying rent for use of its infrastructure. The two companies are the country's largest internet service providers (ISPs), and while Caucasus Online has more subscribers, it is forced to use Georgian Telecom's lines to deliver service. Georgian Telecom cut off service to Caucasus Online users as a result of the dispute, forcing more than 150,000 internet subscribers to switch to its own service.[6]

The Georgian National Communications Commission (GNCC) is the country's main regulatory body, and although there have yet to be many test cases, it seems to be fair in dealing with internet companies. However, there is no significant difference between GNCC procedures for handling traditional media and those pertaining to telecommunication and internet issues, so the criticisms that the GNCC has encountered with respect to its lack of transparency and licensing

[5] "Russian and Georgian websites fall victim to a war being fought online as well as in the field," RSF, August 18, 2008, http://www.rsf.org/article.php3?id_article=2_8167 , accessed March 23, 2009

[6] "Rights of Subscribers Are Sacrificed to the Controversy between Caucasus Online and United Telecom," HumanRights.ge, October 24, 2008, http://www.humanrights.ge/index.php?a=article&id=3246&lang=en , accessed March 20, 2009

procedures for traditional media may reappear in the context of the internet. Indeed, the regulator's failure to react promptly to the 2008 corporate dispute described above highlighted its inability to cope with fast-moving problems in the private sector.

Limits on Content

Government censorship is not a major hindrance to internet freedom in Georgia, though there have been some exceptions. Georgian internet users can freely visit any website around the world, upload or download any content, and contact other users via forums, social networks, and applications like instant messaging. In fact, content is so accessible that numerous sites offer illegal material such as pirated software, music, and movies, and the government has not enacted appropriate legal measures to limit illicit content. Within state institutions there is a small degree of mandated censorship, and the traffic and content is filtered for material like pornography and unlicensed software, but there is no official law or order regarding this practice. The government apparently does possess the capacity to block content on a larger scale, however, as evidenced by its actions in August 2008. While access to some social-networking sites with the .ru country code was restored fairly quickly, the block on Russian news sites stayed in effect until the end of September,[7] and forum.ge, one of Georgia's biggest discussion forums, was closed down for about five weeks. The decision to filter and censor was taken by the executive branch alone and lacked judicial oversight and other procedures that would have enabled public input or transparency. There was no clear legal basis for the action.

Many news sites and services were launched in 2008, which should result in the continued popularization of the internet as a source of information. However, in a spillover effect from traditional media, which operate in a harsher and less free environment, internet journalists are rarely critical and generally do not ask pointed questions of the government, politicians, or other institutions. Unlike bloggers, who write about daily life or professional issues, journalists who publish online report a high level of pressure from the authorities to practice self-censorship. Consequently, some write under pseudonyms, while others keep private blogs. From time to time online journalists complain that "someone" has tried to force them not to write or discuss particular topics. The state of emergency declared in November 2007, which resulted in temporary press and television censorship, was a particular boost for internet use, as many journalists and news agencies began to pay more attention to the medium. Multiple blogs and news sites were created to deliver news during the press and broadcasting blackout. Similarly, during the 2008 conflict with Russia, restrictions on content were circumvented fairly easily, as many state employees and even official press services of governmental bodies switched to free blogging platforms to publish their points of view as well as official announcements.[8]

There are about 50 bloggers writing in the Georgian language who try to remain active and current. However, at this point the blogosphere is still very weak. Traditional media still have a much stronger presence in society than new media, as every new social or political activity is widely screened on television and discussed in the newspapers, while the internet is viewed more as a source of entertainment or as a place to state contesting opinions. Minorities are not restricted from internet use, but they are represented online through only a small number of forums and blogs. Likewise, civil society groups do not have a significant presence online.

[7] "Georgia cuts access to Russian websites, TV news," Reuters, August 19, 2008, http://www.reuters.com/article/internetNews/idUSLJ36223120080819?pageNumber=2&virtualBrandChannel=0&sp=true , accessed March 26, 2009

[8] Ministry of Foreign Affairs Georgia, http://georgiamfa.blogspot.com/ and State Minister for Reintegration, http://stateminister.blogspot.com/ , accessed March 20, 2009

Mobile phones are not widely used for social or political mobilization. However, in August 2008 an anonymous text message was sent to mobile-phone users, urging them to attend a rally in Tbilisi "against Russian aggression and occupation."[9] It is estimated that at least 10,000 people took part in the rally.[10] Mobile phones are already being used to support or deny official versions of events. Users are filming events as they happen and then posting the videos to sharing sites, often capturing images that are not shown on television and providing a more accurate picture of news developments.[11] A group of volunteers launched the country's first internet television channel in November 2008, possibly in an effort to fill the gap left by the shutdown of the opposition-oriented television station Imedi in late 2007. Due to technical problems the new channel is currently unable to carry live broadcasts and instead replays "archived footage of various television channels, footage taken by mobile phones and reports done by independent reporters."[12]

Violations of Users' Rights

Civil rights including the right to access information and freedom of expression are guaranteed by the Georgian constitution, and they are generally respected in practice. There are no specific laws that directly address online activity. However, the Law on Freedom of Speech and Expression "makes it clear that other 'generally accepted rights' related to freedom of expression are also protected even if they are not specifically mentioned."[13] At the same time, while there have been no cases to date, internet activities can be prosecuted under that law—mainly for defamation—or under any applicable criminal law. The judiciary has been unable to establish itself as an independent institution, and it continues to suffer from extensive corruption and pressure from the executive branch, though this has yet to play out in internet-related cases.[14]

Surveillance is not pervasive, and anonymous communication is allowed. However, in certain cases and under government orders, ISPs are obliged to deliver statistical data—separated by user—about site visits, traffic, and other topics. Mobile-phone companies are required to provide similar data when asked by the government. Cybercafes are not obliged to comply with government monitoring, as they do not register or otherwise gather data about users, and users are not forced to provide personal information in order to access the internet. People are not required to register when they buy a mobile phone, but registration is needed to buy a SIM card and obtain a number.

There have been no documented cases of extralegal intimidation or physical violence against online journalists, bloggers, or other information and communication technology (ICT) users. However, cyberwarfare was waged by Russian hackers against government websites during the August 2008 conflict. The websites of the parliament and the ministry of foreign affairs were knocked out for a few days, and hackers posted defamatory images of the Georgian president in their place. Georgia's ISPs also came under attack, and mobile internet services were affected by problems in the phone network, which was overloaded with calls.[15]

[9] "Anonymous SMS message calls for mass rally in Tbilisi," Agence France-Presse, August 10, 2008, 2:26 pm
[10] "Thousands rally in Tbilisi against Russia," Agence France-Presse, August 10, 2008, 7:06 pm
[11] For example, this video showing masked supporters of government (presumably policemen or state security staff) shouting against opposition rally - http://www.myvideo.ge/?video_id=82554
[12] "Georgia launches internet TV channel," Agence France Presse, November 7, 2008 - (www.gevision.tv)
[13] Guide to the Law of Georgia on Freedom of Speech and Expression, http://www.article19.org/pdfs/analysis/georgia-foe-guide-april-2005.pdf, accessed March 17, 2009
[14] Freedom of the Press - Georgia (2008), http://www.freedomhouse.org/template.cfm?page=251&year=2008
[15] Global Voices Online, "Blogging the War," August 28, 2008, http://globalvoicesonline.org/2008/08/28/georgia-blogging-the-war/, accessed March 17, 2009

India

Status: Partly Free

Obstacles to Access: **11** (0–25)
Limits on Content: **8** (0–35)
Violations of User Rights: **15** (0–40)
Total Score: **34** (0–100)

Population: 1.1 billion
Internet Users/Penetration 2006: 40 million / 4 percent
Internet Users/Penetration 2008: 82 million / 7 percent
Mobile Phone Users/Penetration 2006: 166 million
Mobile Phone Users/Penetration 2008: 347 million
Freedom of the Press (2008) Score/Status: 35 / Partly Free
Digital Opportunity Index (2006) Ranking: 124 out of 181
GNI Per Capita (PPP): $2700
Web 2.0 Applications Blocked: No
Political Content Systematically Filtered: No
Bloggers/Online Journalists Arrested: Yes

Introduction

New media took hold in India during the mid-1990s, with mobile-phone services and commercial internet connections first made publicly available in 1994 and 1995, respectively.[1] These services expanded rapidly in the late 1990s, with an increasing number of mobile service providers entering the Indian market, as well as with the opening up of the internet-service provider (ISP) sector in 1998 through the Central Government's New Internet Policy.[2] Most major public encounters with state-driven attempts to monitor and regulate access to these technologies began during the first half of the current decade. Internet freedom in India faces threats, however, particularly due to increasing state regulation in response to the authorities' rising abilities to control the internet, as well as regulation by different private interests and local political groups.

Obstacles to Access

Infrastructure limitations and cost considerations restrict access to the internet and other information and communication technologies (ICTs) in India. Though regarded by some as the country with the fourth-highest number of internet users globally, the degree of internet penetration in India is low. Although the actual figures are disputable given that different sources have presented different findings,[3] the cited figure of 82 million internet users in India pales in comparison to the total population, representing a maximum penetration rate of approximately 6.9 percent of the population.[4] Within this, there is a pronounced urban-rural digital divide, with the approximate rural user base only 5.5 million. Thus, on average, there are at least ten times more urban internet users than rural internet users in India.[5] While approximately 37 percent of India's internet users access

[1] *See* Access Denied: The Practice and Policy of Global Internet Filtering 287 (Ronald Deibert et al eds. 2008) [hereinafter referred to as 'Open Net Initiative - Access Denied: India Profile'], *and* Cellular Operators Association of India, *History of Cellular Telephony in India*, at http://www.coai.com/historyIndia.php.
[2] *See* Vikram Raghavan, Communications Law in India 472-473 (2007)
[3] C.P. Chandrashekhar, *India is Online but Most Indians are Not*, Macroscan, (September 26th, 2006), http://www.macroscan.org/the/services/sep06/ser260906India_Online.htm
[4] ITU, http://www.itu.int/ITU-D/icteye/Default.aspx
[5] IAMAI & IMRB, *I-Cube 2008: Internet in India – Summary Report*, at http://www.iamai.in/Upload/Research/I-Cube_2008_Summary_Report_30.pdf, accessed December 2008

the internet via cybercafes, the number accessing the internet from home computers has increased.[6] Low literacy rates are also a major obstacle in permitting many Indian citizens to use the internet, especially in rural areas.[7] Though growing, the availability of internet content in India's eight most widely-spoken languages is poor, with the current number of local language websites as low as 1,500.[8]

The overall mobile phone penetration figures are much better, with around 31 percent of the population using mobile phones, and the total national mobile subscriber base estimated at 347 million.[9] Despite the global economic crisis and the high level of poverty in India, the mobile phone market continues to increase at an astonishing rate; statistics indicate that in September 2008, India's mobile market grew at the rate of four new phone subscribers every second.[10] While Indians use SMS messaging as a feature of their mobile phones, the number of messages is generally lower than in surrounding countries due to higher taxes on SMS messages. Since the deregulation of the telecom and ISP sectors in the late 1990s, users in India have had a choice between a number of different public and private providers. Bharat Sanchar Nigam Limited (BSNL; a state-owned public enterprise) and Videsh Sanchar Nigam Limited (VSNL; formerly state-owned and now privately-owned) are the two service providers with the most dominant market share, followed by wholly private service providers such as Sify Limited, Bharti Infotel, and Reliance Communications, among others.[11]

By and large, there has been no sustained government policy or strategy to block access to most categories of internet technologies or digital applications. Attempts to filter content have originated at the level of executive action by state governments, as well as by private individuals through court cases. Such attempts have focused on ordering ISPs to block access to social networking websites such as Orkut due to concerns about content,[12] as well as to block access to Google Earth due to national security concerns.[13] In November 2008, Indian authorities reportedly asked citizen journalists to stop updating their Twitter accounts with information on the Mumbai terrorist attacks, arguing that the posts were creating a security threat.[14] There is currently no sustained blocking of entire online media services or blogging platforms; the widespread blocking of Geocities in 2003 and blogging platforms in 2006 were the result of over-blocking by ISPs in the

---

[6] *Id.*

[7] *See* IAMAI & IMRB, *supra* note 4

[8] IAMAI & IMRB, *Vernacular Content Market in India Report,* at http://www.iamai.in/Upload/Research/Vernacular%20Content%20Report_29.pdf, accessed December 2008

[9] ITU, http://www.itu.int/ITU-D/icteye/Default.asp

[10] "India, 4 new mobile phone subscribers every second," *Textually.org*, October 22, 2008, http://www.textually.org/textually/archives/2008/10/021533.htm, accessed December 2008

[11] *See* Telecom Regulatory Authority of India, TRAI Annual Report for 2006-07 63 (available at http://www.trai.gov.in/annualreport/AReport2006-07English.pdf)

[12] See *Google's social networking site in trouble*, The Times of India (2006), http://timesofindia.indiatimes.com/articleshow/2136970.cms, accessed December 2008 *and* Amit Varma, *Orkut and censorship in India*, India Uncut (2007), http://indiauncut.com/iublog/article/orkut-and-censorship-in-india/, accessed March 30, 2000. *See also* Open Net Initiative - Access Denied: India Profile, at 289-291

[13] See *PIL asking Google to remove India from Google Earth*, pluGGd.in (2008), http://www.pluggd.in/india-internet/pil-asking-google-to-remove-india-from-google-earth-3305/, accessed March 30, 2009, *and* Rhys Blakely, *Indian court asked to ban Google Earth*, Times Online (2008), http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article5314085.ece, accessed March 30, 2009. *See also* J.Mohanraj vs The Secretary to Government (Home), Madras High Court Writ Petition No.29713 of 2008, decided on 17 December, 2008 (available at http://www.indiankanoon.org/doc/1191397/) (holding that the Madras High Court could not grant a public interest litigation plea to ban Google Earth).

[14] *Times Online*, "Citizen journalists told to stop using Twitter to update on Bombay attacks," November 27, 2008, http://technology.timesonline.co.uk/tol/news/tech_and_web/article5245059.ece, accessed March 30, 2009

process of carrying out the government-mandated filtering of specific sub-domains, causing the collateral blocking of entire websites.[15] In May 2008, the central government threatened to ban Research-in-Motion's Blackberry service from continuing to operate in India due to the firm's refusal to facilitate the interception and decryption by Indian government agencies of information communicated across its network.[16]

The Telecom Regulatory Authority (TRAI) of India is the main regulatory body with respect to telecommunications matters; however, the scope of its regulatory power over internet matters in India is somewhat unclear given that the Ministry of Telecommunications and Information Technology, along with the Ministry of Home Affairs, also exercise control over several aspects of internet regulation. TRAI functions as an independent regulator with public consultations and other participatory decision making processes, while the Ministry of Telecommunications and Information Technology and the Ministry of Home Affairs function as government departments tied to the ministerial structure of the central government.

Limits on Content

Prior to 1999–2000, the then state-owned company VSNL had a monopoly in the ISP sector and sporadically filtered internet content. The two main publicly-known instances during this time pertained to blocking access to the website of *The Dawn*, a Pakistani newspaper, for the duration of the Kargil conflict.[17] Since 2003, the institutional structure of internet censorship and filtering in India has centred around the Indian Computer Emergency Response Team (CERT-IN), a body within the Department of Information and Technology. This body was created by a 2003 executive notification to be a nodal agency for accepting and reviewing requests from a designated pool of government officials to block access to websites. When CERT-IN decides to block a website, it directs the Department of Telecommunications to order all Indian ISPs licensed by it to comply with this order.[18] Among the noteworthy instances of such blocking was the Yahoo! group Kynhun (linked to the Hynniewtrep National Liberation Council) in 2003, and 17 various websites and blogs in 2006.

Police agencies in different states have also played a role in attempting to mandate internet censorship and surveillance, most notably in the state of Maharashtra.[19] Instances in which websites and blogs were blocked due to national security, secessionist, and hate speech threats took place in

[15] *See* Open Net Initiative - Access Denied: India Profile, at 290. *See also* Sandeep Dikshit, *Bid to block anti-India website affects users*, The Hindu (2003), http://www.thehindu.com/2003/09/23/stories/2003092312761100.htm, accessed March 30, 2009, and Editorial Opinion, *Censorship of Internet*, The Hindu, (2003), http://www.thehindu.com/2003/10/21/stories/2003102101231000.htm, accessed March 30, 2009. Shivam Vij, *Blog blockade will be lifted in 48 hours*, Rediff News (2006), http://www.rediff.com/news/2006/jul/19blogs.htm, *and* Shivam Vij, *Possible action against ISPs for blocking sites*, Rediff News (2006), http://www.rediff.com/news/2006/jul/20dot.htm.

[16] *Blackberry spurns Indian spy call*, BBC, May 27, 2008, http://news.bbc.co.uk/2/hi/south_asia/7420911.stm, accessed March 30, 2009. *See also* Press Trust of India, *India backs DoT on Blackberry; asks RIM to cooperate*, The Times of India, (May 11 2008), http://timesofindia.indiatimes.com/Business/India_Business/India_backs_DoT_on_BlackBerry_asks_RIM_to_cooperate/articleshow/3030151.cms, *and* Ketan Tanna, *Outsmarting Big Brother*, The Times of India, (June 8 2008), http://timesofindia.indiatimes.com/Sunday_Specials/Outsmarting_Big_Brother/articleshow/3110252.cms.

[17] *See* Farzad Damania, *The Internet: Equalizer of Freedom of Speech? A Discussion on Freedom of Speech on the Internet in the United States and India*, 12 Indiana International & Comparative Law Review 243, 259 (2002).

[18] *See* Open Net Initiative - Access Denied: India Profile, at 290. *See also* Raman Jit Singh Chima, *The Regulation of the Internet with relation to Speech and Expression by the Indian State* 32-36, 53-54(April 25, 2008). Available at SSRN: http://ssrn.com/abstract=1237262.

[19] *See* Open Net Initiative - Access Denied: India Profile, at 288-289. *See also* Chima, *supra* note 16, at 55-58.

2003 and 2006, but were disjointed in their technical operation and were more event-specific in nature.[20] There has been no sustained state-mandated process of internet censorship or blocking, though some reports indicate that more sophisticated filtering mechanisms are being installed at the level of ISP gateways at the instruction of the central government.[21]

The Indian blogosphere is quite active, complimenting the rise in internet use by different interest groups as well as by civil society actors. The actual number of bloggers, though, still appears to be quite low, and the blogosphere is potentially fragmented given the large number of blogging platforms available.[22] Online communication and social networking services are increasingly being used as means to organize politically, as evidenced by prominent instances such as the meetings and rallies organized to protest the November 2008 terrorist attacks in Mumbai, the outcry against the blocking of blogging platforms in 2006, and social mobilization movements such as Blanknoise, among others.[23] Bloggers utilized the internet to voice concern and frustration over the inadequacy of government security capabilities after terrorist attacks throughout 2008, questioning that bombings were becoming a regular occurrence in India and predicting which city would fall victim next.[24] There was also extensive debate on the blogosphere over attacks on Christians by groups of radical Hindu nationalist rioters in various Indian states.[25]

Violations of Users' Rights

Article 19(1)(a) of the Constitution explicitly protects the right to freedom of speech and expression, subject to reasonable restrictions that the state can impose. However, its application vis-à-vis internet content has not yet been directly clarified by a judicial ruling, though positive remarks regarding its applicability have been made in passing in cases decided by the Bombay High Court and the Supreme Court of India.[26] Article 19(1)(a) has also been held to apply—along with the right to life and liberty under Article 21—to the privacy of telephone communication, with guidelines established regulating the ability of state officials to intercept communication under the broad power granted to them by the Telegraph Act.[27]

The legal landscape for internet communication is laid out by statutes such as the Telegraph Act, the Indian Penal Code, the Code of Criminal Procedure, and the specialized provisions of the Information Technology Act (ITA). The ITA, enacted in 2000, was extensively amended by

[20] *Id.*
[21] Indrajit Basu, *Security and Censorship: India to Clip the Wings of Internet*, GovTech (2007), http://www.govtech.com/gt/articles/103332, accessed March 30, 2009.
[22] Frederick Noronha, *Blogging: Can ICTs Really Make Free Speech a Reality in India?*, Indiablogs, (February 02, 2006), http://indiaweblogs.blogspot.com/2006/02/blogging-can-icts-really-make-free.html, accessed March 30, 2009. *See also Blogging India: A Windows Live Report* (Press release with summary of findings available at http://download.microsoft.com/download/d/3/b/d3b7d5c9-6005-434c-8e71-822678b15eac/pr_271106.doc).
[23] See Claudine Beaumont, *Mumbai attacks: Twitter and Flickr used to break news*, Telegraph.co.uk, November 27, 2008, http://www.telegraph.co.uk/news/worldnews/asia/india/3530640/Mumbai-attacks-Twitter-and-Flickr-used-to-break-news-Bombay-India.html, accessed March 30, 2009; *and* Rachel Dixon, 2008's Top 10 Moments in User-Generated News: Mumbai Attacks, NowPublic, (December 15, 2008), http://www.nowpublic.com/tech-biz/1-mumbai-attacks-2008-review, accessed March 30, 2009. *See also* Pramod K. Nayar, *India goes to the blogs: Cyberspace, identity, community*, in Popular Culture in a Globalised India 207 (2009), and http://blog.blanknoise.org/
[24] Global Voices Online, "A Turbulent Year for South Asia," December 27, 2008, http://globalvoicesonline.org/2008/12/27/2008-a-turbulent-year-for-south-asia/, accessed March 30, 2009
[25] *Id.*
[26] Archana Tyagi et al, *Report of the Committee Appointed by the Bombay High Court in Suo Motu Writ Petition No. 1611 of 2001 to Recommend Measures to Protect and Shield Minors from Pornographic and Obscene Material on the Internet* 1 (2002), *available at* http://www.cyquator.com/html/vol1.pdf, *and* Ajay Goswami v. Union of India (2007) 1 SCC 143
[27] PUCL v. Union of India (1997) 1 SCC 301. *See* also Raghavan, *supra* note 2, at 760-761

Parliament in December 2008 in three significant ways. First, it penalizes those who refuse orders from authorized state agencies to intercept or decrypt information. Most notably granting legislative sanction to the central government's power to order that a website be blocked. It may be argued that the grounds listed in the amended law for the exercise of this power do not conform with the constitutionally permissible restrictions on the right to free speech listed by Article 19(2).[28] Secondly, these amendments have considerably broadened the scope of activity criminalized by the statute, in particular: sending messages deemed offensive, dishonestly receiving stolen computer resources or communication devices, identity theft, impersonation, violation of bodily privacy, cyberterrorism, the publication or transmission of sexually explicit material, and child pornography.[29] Finally, the amendment strengthens the immunity of network intermediaries (a category that can be roughly held to cover both ISPs and online service providers) from prosecution for offences under the statute, although to a lesser extent than the wide safe harbour rule that was originally intended to be introduced.[30] This immunity to network intermediaries was created in response to the high profile prosecution of the CEO of Bazee.com (now eBay India) by the Delhi Police for a controversial sexually explicit video clip uploaded via the service. On appeal, the Delhi High Court upheld its ruling (released before the ITA Amendment Bill was passed) that a case could in fact be made for intermediary liability for obscene content under the statute.[31] The substantive trial in the case is yet to be completed, however. The amended position in the ITA vis-à-vis the exemption of intermediaries from liability removes the burden of proof from intermediaries.[32] It is important to note that this amendment necessitates not only that service providers act when informed about their involvement in unlawful acts by state agencies, but that they must also observe guidelines that the central government might prescribe as to the due diligence they have to discharge.[33] These guidelines have not yet been publicly framed or notified. Overall, there seem to be few regular prosecutions under this statute, with 2006–2007 figures showing 99 cases registered with police units regarding the transmission of obscene content, and two cases regarding the failure of parties to comply with decryption as per the pre-amendment statute.[34]

The regulations found in the ITA may oblige companies to give up the names of individual users to demonstrate their own innocence and a company is presumed responsible for the content posted on the websites it hosts unless it can prove that it was not aware of the content posted by an individual user.[35] As a result, internet bloggers have individually experienced prosecution by Indian authorities for online postings. In May 2008, two men were arrested and charged under both the Indian Penal Code and the Information Technology Act for posting derogatory comments about Congress chief Sonia Gandhi on a community on the social networking site Orkut. While the text

---

[28] *See* Section 69A of the amended Information Technology Act, and Chima, *supra* note 16, at 32-36

[29] See Sections 66A, 66B, 66C, 66D, 66E, 66F, 67A, and 67B of the amended Information Technology Act

[30] Information Technology Amendment Bill, 2008 (available at http://164.100.24.219/BillsTexts/LSBillTexts/PassedLoksabha/96-c%20of%202006.pdf). A summary of the previous version on the amendment bill is available at http://www.prsindia.org/docs/bills/1192012012/1192012012_96_2006.pdf and the report of the Parliamentary Standing Committee whose comments seem to be the reason why the amendment was changed is available at http://164.100.24.207/committeereports/Information%20Technology/REPORT-I.T.-50E.pdf

[31] Avnish Bajaj. v. State, Delhi High Court, decided on May 29th, 2008 (available at http://www.indiankanoon.org/doc/309722/)

[32] Section 79 of the amended Information Technology Act

[33] *Id.*

[34] National Crimes Record Bureau, Crime in India Table 18.4 (2008) (available at http://ncrb.nic.in/cii2007/cii-2007/Table%2018.4.pdf)

[35] "Bombay High Court: orders Google's subsidiary to reveal identity of blogger after posting critical comments," IFEX, August 26, 2008, http://www.ifex.org/en/content/view/full/96437, accessed March 30, 2009

was posted on a community entitled "I hate Sonia Gandhi", the person who formed the community did not face charges as voicing a personal dislike is protected in India under freedom of choice.[36] Google, owners of Orkut, accommodated the authorities' request for the poster's identity.[37] Authorities have subsequently ordered Google to disclose additional bloggers' personal information for other court cases in India, including defamation suits.[38]

The exact shape and extent of surveillance of both internet communication and mobile-phone networks in India is currently unclear. Wire intercepts of telephone conversations are allowed under the guidelines prescribed by the Supreme Court,[39] and their admissibility as evidence in a court of law is not constrained by the legality of the process in which such evidence was procured.[40] The extent and level of sophistication of state surveillance of internet communication in India is unknown, though anecdotal accounts indicate that the government's Intelligence Bureau began using a keyword-based interception system in addition to targeted-IP address interception as far back as 2001.[41] There is no requirement for prior judicial approval before intercepting communication either under the Telegraph Act or the ITA, and the post-amendment ITA grants both central and state governments the power to issue directions for the interception, monitoring, or decryption of computer information, while leaving the prescription of procedure and safeguards for the exercise of such powers to the government itself.[42] It also grants the central government the power to mandate the preservation and retention by intermediaries of such information, and makes the contravention of such orders an offence.[43] The monitoring and collection of traffic data by a government agency for the purposes of enhancing cybersecurity and network protection is also a power vested in the central government to exercise according to the amended statute.[44]

Cybercafes are regulated across most Indian states; the exact extent and manner of regulation varies according to the policies of the different state police forces concerned, but largely focus on the elimination of anonymous access by mandating the recording of certain basic user details in registers as a minimum requirement.[45] Some cybercafes may request a passport photo for their records or demand specific reasons for visiting cybercafes outside their localities.[46] With respect to mobile phones, the Department of Telecommunications has instructed operators to only issue and activate mobile SIM cards after users register their personal details with these companies; the rationale being that this helps ensure national security by preventing terrorists from easily securing anonymous access to SIM cards.[47] This system has been in place for some time, but became the subject of increased emphasis and oversight after the November 2008 Mumbai attacks, with the

[36] *The Times of India*, "One Held for Posting Obscene Orkut Message on Sonia," May 19, 2008
[37] Global Voices Online, "Google Assists Police in Orkut User's Arrest," May 22, 2008, http://advocacy.globalvoicesonline.org/2008/05/22/india-google-assists-police-in-orkut-users-arrest/, accessed March 30, 2009
[38] "Google ordered to reveal blogger's identity," August 15, 2008, http://committeetoprotectbloggers.org/2008/08/15/google-ordered-to-reveal-bloggers-identity/, accessed March 30, 2009
[39] *Supra* note 23.
[40] *See* State (NCT of Delhi) v. Navjot Sandhu 2005(11) SCC 600
[41] Siddarth Srivastava, *India: E-mail users beware, Big Brother is watching*, The Times of India, (December 24, 2001), http://www.blythe.org/nytransfer-subs/Covert_Actions/India:_E-mail_users_beware,_Big_Brother_is_watching, accessed March 30, 2009
[42] Section 69(1) of the amended Information Technology Act
[43] Section 67(C) of the amended Information Technology Act
[44] Section 69B of the amended Information Technology Act
[45] *See* Chima, *supra* note16, at 37-41
[46] *The Times of India*, "ID proof must for cyber café users," August 18, 2008
[47] Special Correspondent, *Centre to enforce SIM card verification process by cell phone operators*, The Hindu, (December 26, 2008), http://www.hindu.com/2008/12/26/stories/2008122655831200.htm, accessed March 30, 2009

central government not only castigating mobile operators on their implementation of the verification process, but also reportedly asking them to disconnect all handsets that do not have international mobile equipment identity (IMEI) numbers.[48]

There have been past incidents involving service attacks and the hacking of websites by nonstate actors during incidents of cross-border tension with Pakistan and China,[49] particularly between 1998 and 2002, and during 2008.[50] Thus far, however, online journalists and bloggers have not been victims of physical attacks.

[48] Rashmi Pratap, *DoT asks cellcos to cut off handsets without IMEI code*, The Economic Times, December 19, 2008, http://economictimes.indiatimes.com/News/News_By_Industry/Telecom/DoT_asks_cellcos_to_cut_off_handsets_without_IMEI_code/rssarticleshow/3859301.cms, accessed March 30, 2009

[49] See Reporters Without Borders, Internet Under Surveillance 2004 – India, at http://www.rsf.org/article.php3?id_article=10750&Valider=OK, accessed March 30, 2009

[50] Aasis Vinayak, *The other Indo-Pak war*, Sify News (January 12, 2009), http://sify.com/news/fullstory.php?id=14835651, accessed March 30, 2009

Iran

Status: Not Free

Obstacles to Access:	**19** (0–25)
Limits on Content:	**24** (0–35)
Violations of User Rights:	**31** (0–40)
Total Score:	**74** (0–100)

Population: 72.2 million
Internet Users/Penetration 2006: 18.2 million / 26 percent
Internet Users/Penetration 2008: 23 million / 32 percent
Mobile Phone Users/Penetration 2006: 15.4 million
Mobile Phone Users/Penetration 2008: 30.2 million
Freedom of the Press (2008) Score/Status: 85 / Not Free
Digital Opportunity Index (2006) Ranking: 105 out of 181
GNI Per Capita (PPP): $10,800
Web 2.0 Applications Blocked: Yes
Political Content Systematically Filtered: Yes
Bloggers/Online Journalists Arrested: Yes

Introduction

Although Iranians are active readers and producers of online content, the Iranian regime wields one of the world's most sophisticated apparatuses for controlling the internet and other digital technologies. Internet use in Iran began in 1995 at universities, then spread quickly via internet cafes to an otherwise isolated population with limited access to independent sources of news and entertainment. The government's censorship of the medium did not begin until 2001, but users today operate in an environment that features filtering of content—particularly domestically produced political news and analysis—together with intimidation, detention, and torture of bloggers, online journalists, and cyberactivists. As with restrictions on press freedom that date to the early days of the 1979 revolution, the Islamic Republic couches its restrictions on internet freedom in an opaque and arbitrary conception of Islamic morality outlined by the constitution, the press law, and the penal code.

Obstacles to Access

While the number of internet and mobile-phone users continues to grow, state-imposed and other infrastructural restrictions significantly constrain Iranians' ability to fully access these technologies and related applications. Estimates of Iranian internet users range from 18 to 23 million[1] in a country of just over 70 million people, putting the user penetration rate at over 25 percent. Most Iranians use dial-up service to access the internet via some 24 million land-line telephones and approximately 3,000 internet hosts. Over 1,000 internet cafes operate in Tehran alone, though intermittent government raids lead to temporary closures. Internet cafe owners must register with the Ministry of Communication and Information Technology (MCIT).[2] Mobile phones outnumber land lines, with some 29 million mobile phones in use in 2007, according to the International Telecommunications Union (ITU). Despite the large number of users in urban areas, the high cost of dial-up access at home—particularly in rural areas—and at internet cafes makes the internet prohibitively expensive for most Iranians.

[1] See http://www.itu.int/ITU-D/icteye/Indicators/Indicators.aspx# for statistics on fixed and mobile phone subscribers and number of internet users compiled by the ITU.
[2] http://xn-----btdb4d0zorfa.iranictnews.ir/T_____.htm,

Use of high-speed internet was rapidly gaining ground until October 2006, when connection speeds above 128 kilobits per second were restricted by the MCIT.[3] Observers noted that the limitation would make it more difficult for users to access, download, or share audio, video, and other large files. Universities and research institutions are now permitted to have fast connections, if approved by the MCIT, but internet cafes and home users are limited to the slower speeds. A small, wealthy minority of Iranians use satellite internet connections, which are free of any restrictions by the government. Social-networking sites such as Facebook are largely blocked; in the early days of the internet in Iran, the networking site Orkut gained significant membership before it was banned. The video-sharing site YouTube has been blocked intermittently since December 2006 but remains popular, including for coverage of political protests. Blogging sites such as Blogger and Persianblog are also blocked. The government, which is the sole provider of mobile-phone services, has been known to cut off access for political reasons. On June 27, 2007, after a day of protests over the state's gasoline-rationing program, the government cut off SMS (text messaging) service to Tehran overnight in an effort to prevent the organization of additional demonstrations.[4]

The Iranian government restricts access and content through a mutually reinforcing set of decrees, legal regulations, and institutions. Supreme Leader Ali Khamenei first asserted control over the internet through a May 2001 decree and subsequent legislation by the Cultural Revolution High Council that forced all internet service providers (ISPs) to end their direct connections, obtain a license to operate, and purchase their bandwidth from government-controlled Access Service Providers (ASPs).[5] There are at least a dozen ISPs in Iran, the largest and oldest of which, Pars Online, is partly owned by the government. The mobile phone sector, previously a monopoly controlled by the government-owned Telecommunication Company of Iran (TCI), has opened considerably since 2006 with the entry of MTN Irancell into the market (although MTN Irancell is a private operator, its majority stake is held by a state-owned company). Further market liberalization is planned with the selling of TCI shares to private investors and the granting of additional mobile phone service provider licenses.[6] Competition has led to a significant rise in mobile phone ownership and usage over the past two years, with phones being used to send and receive SMS and photos, and to a lesser extent to access news and connect to the internet.[7]

Multiple government bodies deal with licensing and other regulatory issues. The Ministry of Islamic Culture and Guidance (MICG) is responsible for providing licenses for websites and blogs. The Committee in Charge of Determining Unauthorized Websites (CCDUW) is legally empowered to identify sites that carry forbidden content and report that information to the MCIT for blocking.[8]

Limits on Content

The Iranian government conducts some of the world's most extensive censorship of online content, particularly on issues of political and social reform. Nevertheless, users circumvent filtering and make use of temporary openings in subversive, innovative ways. Both online and offline expression can draw punishment if it is seen as insulting Islam, criticizing religious leaders and institutions,

---

[3] http://www.ict.gov.ir/forum/Default.aspx?g=posts&t=327, and http://www.dw-world.de/dw/article/0,,3705926,00.html

[4] "Iran bans negative petrol stories," BBC News, June 28, 2007, http://news.bbc.co.uk/2/hi/middle_east/6249222.stm

[5] ONI report, Iran, http://opennet.net/research/profiles/iran, accessed March 16, 2009.

[6] "Telecom Stakes Up for Grabs," Iran Daily, http://www.iran-daily.com/1387/3317/html/economy.htm, accessed March 16, 2009.

[7] "Below Government Radar, Iranians Share Information via SMS", at http://www.audiencescapes.org/iran-sms-information-sharing/, accessed March 23, 2009.

[8] ONI report, Iran.

fomenting national discord, or promoting immoral behavior. In late 2008, the government boasted of blocking five million websites, mostly for pornographic content, but also for sensitive political, social, and cultural information.[9] Given the vague language of government blocking directives, many ISPs err on the side of caution by filtering more information than the government may actually require.[10]

International sites devoted to democratic development, freedom of expression, human rights, and civic mobilization are targeted along with domestic websites, and the sites of English-language news sources such as the *New York Times* and the British Broadcasting Corporation (BBC) are sometimes filtered. Reformist websites and blogs are blocked the most frequently, though in some instances the interference is intermittent, perhaps to encourage self-censorship. At the end of 2008, the women's rights website Tagir Bary Barbary (Change for Equality) was blocked for the 18th time in two years, and feministschool.com was blocked for the eighth time.[11] Hard-line and conservative political sites are increasingly being blocked by the authorities as well, as they sometimes present views that diverge from the official line of the Supreme Leader. For example, *Baztab*, a site operated by former Revolutionary Guard commander Mohsen Rezai, was blocked for a few weeks in September 2007,[12] and parliament member Ahmad Tavakoli's *Farda* site, which broke a 2008 scandal in which the newly appointed interior minister was found to have lied about his academic credentials, was also blocked. The government is especially sensitive to internet organizing by student activists, women's rights groups, and ethnic and religious minorities. It blocks, arrests, and otherwise threatens content producers who post news about the statements and organizing activities of these highly mobilized but repressed groups. Sites concerning gays and lesbians are routinely censored, though the Iranian homosexual community has gained an unprecedented voice via the internet (these sites are mostly based abroad), and has publicized the execution of homosexuals. Sites are also hacked and disabled when they become popular or feature politically provocative content.

The Iranian government's strategy for controlling internet content includes three general techniques: automated filtering, manually produced blacklists, and active posting of progovernment information. Automated filtering is enabled by SmartFilter, a commercial content-control software system developed by a U.S.-based firm, though company officials claim that the Iranian authorities are using it illegally and did not purchase it from them. All ISPs are required to install and utilize such government-mandated filtering systems. Automated internet censorship is supplemented by blacklists and blocking directives compiled by various unaccountable government bodies. At the end of 2002, the CCDUW was created to blacklist sites it deems anti-Islamic or a threat to national security. The committee consists of representatives from the Ministry of Information, the MICG, the Broadcasting Agency, the Cultural Revolution High Council, and the Islamic Propagation Organization.[13] Its lists are regularly updated, and ISPs are required to adhere to them and restrict content accordingly, but the lists are not made public.

In May 2006, an office was established at the MCIT in an attempt to centralize state filtering and surveillance efforts, but this effort has not yet fully materialized. Agencies outside the MCIT retain significant de facto power to control the internet, and these entities—including the Supreme

---

[9] "Iran Blocking Access to 5 Million Web Sites," RFERL, November 21, 2008, http://www.rferl.org/Content/Iran_Blocks_Access_to_5_Million_Websites/1351604.html, accessed March 20, 2009.
[10] ONI report, Iran.
[11] "Internet monitored and controlled, even in democracies," RSF, http://www.rsf.org/rubrique.php3?id_rubrique=273, accessed March 20, 2009.
[12] "Offices of website closed, IFEX, September 24, 2007, http://www.ifex.org/en/content/view/full/86497, accessed March 20, 2009.
[13] ONI report, Iran.

Leader's office and the office of Tehran chief prosecutor Saeed Mortazavi—arbitrarily target certain sites, bloggers, and cyberactivists. Mortazavi, who has allegedly played a direct role in the torture of online journalists and activists,[14] announced in December 2008 that he had established a "special department for internet crimes," which will work closely with the intelligence service to block sites and monitor political messages and organizing.[15]

In addition to censorship, the state counters critical content and online organizing efforts by extending state propaganda into the digital sphere. Blogging sites for state officials such as the Supreme Leader and President Mahmoud Ahmadinejad are also maintained. In late 2008, the government announced its intention to launch 10,000 blog sites to correspond with the 10,000 bases of the Basij, a gang-like paramilitary group responsible for violent attacks against student activists and women's rights organizers, although this rhetoric is yet to be implemented in practice.[16]

Self-censorship is extensive, particularly on political matters, and many bloggers and journalists write under pseudonyms. It is important to note that while the Iranian blogosphere and Iranian news sites do push the bounds of what is acceptable to the regime, the most socially and politically progressive sites are managed and staffed by Iranians living abroad. Since the short-lived era of relative press freedom under President Mohammad Khatami, many online intellectuals and activists have left the country. Iran's best-known bloggers—such as Omid Memarian, Roozebeh Mirebrahimi, and Shahram Rafizadeh—are now writing from foreign cities and have been sentenced to prison in absentia.

Yet despite state efforts, blogging from inside Iran forms a large part of the Persian-language internet, with tens of thousands of writers discussing topics ranging from politics to poetry.[17] During 2008, students in particular used blogging platforms to raise awareness and organize support for environmental issues, and to expose the inappropriate behavior of a university official toward a female student. On both the internet and mobile phones, there are daily doses of satire about regime repression, the faltering economy, and the public's dissatisfaction with congested traffic, air pollution, and inadequate living standards. Antifiltering sites and technologies are banned, but users continue to find and engineer means to circumvent government filtering. BBC Radio, Radio Farda, and Voice of America television all supplement their broadcasting with affiliated websites, and they ensure open access by sending circumvention tools to large e-mail lists. The internet has also provided a key platform for international initiatives—such as Article 19's Persianimpediment.org, Freedom House's *Gozaar*, and *Rooz Online*—that promote freedom of expression and inform the Iranian public on human rights issues.

Most if not all leading civil society organizations and civic movements operate their own websites. A prominent example is the site of the One Million Signatures campaign for women's legal equality. Civic groups also use the internet to organize in ways that are prohibited by the regime. In 2007, underground rap-music groups used the internet to gather hundreds of young fans for an otherwise unpublicized outdoor concert in the town of Karaj, outside Tehran. Because concerts, particularly for Western-style music, are largely prohibited, the event resulted in mass arrests. However, it also garnered a great deal of attention among youth and loosened taboos against live music and large, mixed-gender public gatherings.

---

[14] "Iran: Remove Rights Abuser From Delegation at U.N.," June 22, 2006, http://www.payvand.com/news/06/jun/1211.html, accessed March 20, 2009.

[15] http://www.autnews.us/archives/1387,09,00015035, and http://www.radiofarda.com/content/f1_computer_crimes/477374.html, accessed March 20, 2009.

[16] "Iran's bloggers thrive despite blocks," December 15, 2008, http://news.bbc.co.uk/2/hi/middle_east/7782771.stm, accessed March 20, 2009.

[17] Mapping Iran's Online Public: Politics and Culture in the Persian Blogosphere, April 05, 2008 http://cyber.law.harvard.edu/publications/2008/Mapping_Irans_Online_Public

Violations of Users' Rights

Iranian internet users suffer from routine surveillance, harassment, and the threat of imprisonment for their online activities, particularly those who are more critical of the authorities. The constitution provides for limited freedom of opinion and expression, but numerous, haphazardly enforced laws restrict these rights in practice. The 2000 Press Law, for example, forbids the publication of ideas that are contrary to Islamic principles or detrimental to public rights. The government and judiciary regularly invoke this and other vaguely worded legislation to criminalize critical opinions. A comprehensive 2006 cybercrimes bill would have made ISPs criminally liable for content on sites they carried, but it was never passed by the parliament. A different bill, introduced in July 2008, would make some cybercrimes—promoting corruption, prostitution, and apostasy on the internet—punishable by death.[18] It passed its first reading with a vote of 180 to 29, with 10 abstentions, and was still under consideration at year's end.

Since 2004 the authorities have been cracking down on online activism through various forms of judicial and extrajudicial harassment. A increasing number of bloggers have been intimidated, arrested, tortured, kept in solitary confinement, and denied medical care, while others have been formally tried and convicted. According to Reporters Without Borders, the authorities arrested or questioned 17 bloggers during 2008, seven more than in 2007. Article 514 of the criminal code makes insulting the Supreme Leader punishable by six months to two years in prison, and Article 500 sets a penalty of three months to one year in prison for the distribution of propaganda against the state. Bloggers are typically charged with these offenses, and many practice self-censorship to avoid punishment. Even bloggers writing about art and culture, such as Omidreza Mirsayafi, author of the *Rooznegar* blog, have come under attack. In December 2008, he was sentenced to two years in prison for "insulting" the country's leaders and engaging in "publicity against the government" though his blog focused on Persian music and culture.[19] Scores of women's rights activists associated with the grassroots One Million Signatures movement have voiced their demands online and consequently face routine intimidation, denial of travel abroad, arrest, exorbitant bail sums, and imprisonment, in addition to the blocking of their websites.[13] Labor rights organizers are also subject to violations of their right to free expression online. At the close of 2008, Esmail Jafari was sentenced to five months in prison for blogging about a protest by 20 workers who had been dismissed at a factory in Bushehr.[20] As dissident clerics increasingly use the internet to criticize the regime, they too are being punished. A notable example is the November 2008 sentencing of cleric Mojtaba Lotfi to four years in prison, and a subsequent five years of banishment from the religious city of Qom, for posting Grand Ayatollah Hossein-Ali Montazeri's criticisms of the government.[14]

Privacy rights are generally weak. Mobile-phone users must register and provide personal information upon purchasing a SIM card.[21] The Revolutionary Guard, the police, and the Basij have been known to stop people in public places to screen their text messages for content that is critical of the regime.[22] Regarding the internet, regulations were introduced in 2006 with the aim of further

[18] "Authorities urged to quash 30-month prison sentence imposed on blogger," RSF, December 19, 2008 http://www.rsf.org/article.php3?id_article=29767, accessed March 20, 2009.
[19] Mirsayafi died in prison in March 2009.
[20] "Authorities step up Internet surveillance, cyber-dissident sentenced to five years in prison," RSF, December 11, 2008, http://www.rsf.org/article.php3?id_article=29653, accessed March 20, 2009.
[21] http://iranictnews.ir/archive/1387/10/3/D_89392_____.htm
[22] http://www.roozonline.com/archives/2007/01/post_679.php

undermining online privacy. As part of the regulations, the MICG issued a directive on January 1, 2007, that required all owners of blogs and sites produced in Iran to register with the government by March 1. The directive required site owners to provide personal information and to refrain from specified content. The decree was largely ignored, however, and was deemed useless even by an authority from the MICT.

Kenya

Status: Partly Free

Obstacles to Access:	**10** (0–25)
Limits on Content:	**12** (0–35)
Violations of User Rights:	**9** (0–40)
Total Score:	**31** (0–100)

Population: 38.5 million
Internet Users/Penetration 2006: 1.5 million / 3 percent
Internet Users/Penetration 2008: 3 million / 8 percent
Mobile Phone Users/Penetration 2006: 7.3 million
Mobile Phone Users/Penetration 2008: 11.7 million
Freedom of the Press (2008) Score/Status: 60 / Partly Free
Digital Opportunity Index (2006) Ranking: 153 out of 181
GNI Per Capita (PPP): $1500
Web 2.0 Applications Blocked: No
Political Content Systematically Filtered: No
Bloggers/Online Journalists Arrested: No

Introduction

Use of the internet and mobile telephones is relatively unfettered in Kenya, though a lack of infrastructure, both for the country's international connection and in rural areas, poses a significant obstacle. A majority of the population was unable to access the internet in 2008 due to the high costs involved, but this is expected to change with the finalization of several broadband initiatives in 2009 and the introduction of technology allowing access via mobile phones, which are fairly widespread. Despite improving access to the internet, an amendment to the Kenya Communications Act of 1998, commonly referred to as the Communications Amendment Act, has raised concerns that online censorship and surveillance might also increase in the coming years. The measure was passed by Parliament in December 2008 and was awaiting the president's ratification at year's end.

Obstacles to Access

Access to the internet has been growing in recent years, and there have been no restrictions on advanced applications, but the medium remains beyond the reach of most Kenyans. The latest figures for 2008 indicate that approximately 7.9 percent of the population, or roughly three million people, had access during the year, and the penetration rate has more than doubled over the last two years.[1] The spread of the internet is hampered by a poor telecommunications infrastructure and a lack of electricity, particularly in rural areas. This partly explains the disproportionately high concentration of internet subscribers in two of Kenya's largest cities, Nairobi and Mombasa. Knowledge of information and communication technologies (ICTs) remains relatively low, and within the context of competing priorities, the cost of internet access is exorbitant for poor households, despite significant drops in prices. As of 2008, Kenya relied on expensive satellite systems to connect the country's infrastructure with the global internet, but 2009 will mark the introduction of high-speed fiber optic cables to replace this arrangement.[2] As a result, costs are expected to drop and connection speeds should rise dramatically, making the technology affordable

[1] International Telecommunications Union, http://www.itu.int/ITU-D/icteye/Default.aspx
[2] "Internet: Last piece of fibre-optic jigsaw falls into place as cable links east Africa to grid", *The Guardian*, August 18, 2008, www.guardian.co.uk/technology/2008/aug/18/east.africa.internet accessed on March 26, 2009

and accessible to larger segments of the population. Some estimates anticipate an increase to 10 million users over the next five years.[3]

Mobile-phone penetration is significantly higher than internet penetration rates, estimated at nearly 12 million subscribers in 2008.[4] Moreover, mobile-phone coverage extended to 92 percent of the country. The availability of internet access via mobile phones increased in 2008, as Safaricom, a mobile-phone service provider with 10.1 million users and an 80 percent share of the market, launched internet capabilities in Nairobi in May, with other cities and providers expected to follow in the coming year.[5]

Access to a variety of advanced applications is widespread, with individuals and groups able to engage in free expression of views via e-mail, instant messaging, chat rooms, and blogs. There have been no reports that the government uses control over internet infrastructure to limit connectivity, and Kenyans have free access to the social-networking site Facebook, the video-sharing site YouTube, and the blog-hosting site Blogspot, all of which rank among the 10 most popular sites in the country.[6]

Reform in Kenya's information and communications sector has led to a new licensing framework—part of a regulatory strategy that has seen a shift from licensing based on a bidding process to open, market-based licensing. Competition has been introduced in most segments of the telecommunications market, with the effect of reducing costs and generally improving the quality of services, particularly mobile-phone services. Four mobile operators have rolled out their networks, though Safaricom still dominates the market.

The independence of a regulatory body called the Communications Commission of Kenya (CCK) is technically enshrined in the Communications Act, but most of the commissioners are government appointees and their independence is limited in practice. Under the Communications Amendment Act, the CCK and not the independent and professional Media Council of Kenya (MCK) would be responsible for regulating both traditional and online media.[7] In light of Kenya's recent history, including the banning of live television coverage by the government following the 2007 elections, reservations have been raised regarding the implications for free online speech should the act come into effect. Access providers have formed organizations such as the Kenyan ISP Association and the Kenya Cybercafe Owners to lobby the government for better regulations, lower costs, and increased efforts to improve computer literacy.[8]

Limits on Content

The government does not employ technical filtering or extensive censorship, and citizens are generally able to access a wide range of viewpoints. However, the government engaged in ad hoc

[3] " Kenyan firms scramble for share of internet market", *Daily Monitor*, February 26, 2009, www.monitor.co.ug/artman/publish/business/Kenyan_firms_scramble_for_share_of_internet_market_80502.shtml accessed on March 26, 2009

[4] International Telecommunications Union, http://www.itu.int/ICT-D/icteye/default.aspx

[5] "Kenya's Safaricom says to launch 3G service in April", *Reuters*, April 3, 2008, http://in.reuters.com/article/asiaCompanyAndMarkets/idINL0339992220080403 accessed on March 26, 2009; and "Safaricom launches 3G technology", *Network World*, May 27, 2008, http://www.networkworld.com/news/2008/052708-safaricom-launches-3g.html accessed on March 26, 2009

[6] "The 10 Most Popular Sites in Kenya", *Moses Kemibaro*, March 14, 2008, http://moseskemibaro.com/?p=19 accessed on March 26, 2009

[7] "Government enacts Draconian law to regulate media content, gives authorities broad powers of surveillance", *IFEX*, December 15, 2008, www.ifex.org/en/content/view/full/99330/ accessed on March 26, 2009

[8] "Kenyan cyber café owners get together to lobby government", *Balancing Act News Update*, www.balancingact-africa.com/news/back/balancing-act_96.html accessed on March 26, 2009

efforts during 2008 to limit access to some content, including material related to corruption. In May, there were reports that some government departments were blocking access to the Kenya Anti-Corruption Commission's online whistleblower reporting facility.[9] During the postelection violence in early 2008, there were also indications that the government was willing to monitor and censor both internet and mobile-based content that it felt was "inflammatory."

Though individual internet users generally seem comfortable expressing themselves freely online, mainstream media organizations' online portals and their correspondents practice some self-censorship. In addition, a number of bloggers and internet users reportedly chose their words with particular care during the postelection violence to avoid being victimized.

Print outlets, television, and radio continue to be the main sources of news and information for most Kenyans, though there are increasing efforts to extend mainstream news to online platforms. For example, the television stations Nation TV and KTN have used YouTube to rebroadcast news clips. Mobile phones and e-mail were used for political organization during the election campaign in 2007, and to spread ethnic hate speech both during and after the campaign period.

The internet is becoming an important forum for vibrant political debate among residents as well as Kenyans living abroad. Blogs were a crucial source for current information, images, and opinions following the ban on live television and radio broadcasts between December 30, 2007, and February 4, 2008. In particular, an online citizen journalism initiative called Ushahidi was launched during the postelection violence. Its initial purpose was to catalog incidents of violence using messages sent by ordinary citizens via their mobile phones or the internet, and to use that information to map out the unfolding events.[10] Since then, Ushahidi has been used for "crowd-source" news gathering in South Africa and the Democratic Republic of Congo.[11] Other issues covered by Kenyan bloggers during the year included corporate environmental abuse,[12] accusations of United Nations hypocrisy,[13] and the debate over women's reproductive rights.[14]

Violations of Users' Rights

While the constitution protects freedom of expression and the "freedom to communicate ideas and information," it also grants the government the authority to place restrictions on defamation, privileged information, and state employees "in the interest of defence, public safety, public order, public morality or public health." Criminal defamation laws remain on the books in Kenya, and in 2008 the authorities used them to intimidate journalists working in traditional media, but there do

[9] "The Kenya Anti Corruption Commission & Internet Censorship in Kenya-An Exercise in Futility", *Mars Group Kenya,* May 29, 2008, http://www.marsgroupkenya.org/user/?p=110; http://wikileaks.org/wiki/Anti-corruption_whistleblowing_website_blocked_by_Kenyan_Government accessed on March 26, 2009

[10] *Ushahidi,* www.ushahidi.com/about accessed on March 26, 2009

[11] "Citizen Voices", *Forbes*, December 8, 2008, http://www.forbes.com/free_forbes/2008/1208/083.html accessed on March 26, 2009

[12] "Environment: Dirty Dealings and Water Masses", *Global Voices*, December 1, 2008, http://globalvoicesonline.org/2008/12/01/environment-dirty-dealings-and-water-masses/ accessed on March 26, 2009

[13] "Yellow Humvees and the UN Procurement Scandal", *Global Voices*, November 18, 2008, http://globalvoicesonline.org/2008/11/18/yellow-humvees-and-the-un-procurement-scandal/ accessed on March 26, 2009

[14] "Kenya: Reproductive Rights Bill Sparks Abortion Debate", *Global Voices*, August 28, 2008, http://globalvoicesonline.org/2008/08/28/kenya-reproductive-rights-bill-sparks-abortion-debate/ accessed on March 26, 2009

not appear to have been any cases aimed at online commentators.[15] In a negative development, the Communications Amendment Act was passed in December despite significant opposition from local media workers and international press freedom watchdogs. The measure, if ratified by the president, would give the government broad powers of censorship, including over certain online content.[16] It would also permit the minister of internal security to authorize raids on media houses and confiscation of telecommunications equipment in the name of national security. Other provisions of the act allow for increased retention of data and its use as evidence in court.

During the violence that followed the flawed December 2007 election, the government banned all live radio and television broadcasts and warned Kenyans about circulating news via SMS (text messaging). "The Ministry of Internal Security urges you to desist from sending or forwarding any SMS that may cause public unrest," read a message that was sent to Safaricom users. This suggested that the government had the capability to monitor mobile-phone usage if necessary, but there have been no reports of blocked mobile-phone access. The government also reportedly monitored internet content during the unrest.[17]

There were no reports of extralegal intimidation of journalists, bloggers, or other ICT users by state authorities or any other actor during the coverage period, though the general atmosphere of intimidation and fear surrounding the postelection violence affected online commentators as well as traditional journalists.

[15] "2008 Human Rights Report: Kenya", *U.S. Department of State*, *February 25, 2009,* www.state.gov/g/drl/rls/hrrpt/2008/af/119007.htm accessed on March 26, 2009

[16] "Attacks on the Press in 2008: Kenya", *Committee to Protect Journalists*, www.cpj.org/2009/02/attacks-on-the-press-in-2008-kenya.php accessed on March 26, 2009

[17] "2008 Human Rights Report: Kenya", www.state.gov/g/drl/rls/hrrpt/2008/af/119007.htm accessed on March 26, 2009

Malaysia

Status: Partly Free

Obstacles to Access: **8** (0–25)
Limits on Content: **12** (0–35)
Violations of User Rights: **20** (0–40)
Total Score: **40** (0–100)

Population: 27 million
Internet Users/Penetration 2006: 11 million / 39 percent
Internet Users/Penetration 2008: 15 million / 56 percent
Mobile Phone Users/Penetration 2006: 19.5 million
Mobile Phone Users/Penetration 2008: 23.7 million
Freedom of the Press (2008) Score/Status: 65 / Not Free
Digital Opportunity Index (2006) Ranking: 57 out of 181
GNI Per Capita (PPP): $13,600
Web 2.0 Applications Blocked: No
Political Content Systematically Filtered: No
Bloggers/Online Journalists Arrested: Yes

Introduction

Freedom of the internet and digital media in Malaysia has grown in the past two years, as the government has encouraged increased access, and information and communications technologies (ICTs) have been playing a greater role in political mobilization and participation. The most notable trends have been the growing population of bloggers in the country and the increased use of video-sharing websites, such as YouTube, to spread political messages, especially in the run-up to the country's 12th general election on March 8, 2008. However, this expansion has encountered some obstacles. Several bloggers have been arrested or faced defamation charges under vaguely worded legislation, raising concerns that traditional press freedom restrictions may spill over into cyberspace.

Malaysia's first internet service provider (ISP), Jaring, was inaugurated in 1992 by the Malaysian Institute of Microelectronic Systems[1] (MIMOS), with an initial group of 28 subscribers. The growth of internet in Malaysia has since been steady and incremental, driven in large part by state-guided initiatives that were rolled out every two to three years.

Obstacles to Access

Malaysia has a relatively high degree of internet penetration, with approximately 15 million users—more than half of the total population of 27 million—as of 2008.[2] There are currently 21 ISPs operating in the country, most of them privately owned. The three private mobile-telephone service providers are Maxis Communications, Celcom, and Digi.com, which control 42 percent, 32 percent, and 26 percent of the market, respectively.[3] Malaysians can access the internet through home connections, mobile phones, or cybercafes.

While the country was an early adopter of the internet and has pioneered some of the first ICT regulatory frameworks in the region, especially through the Multimedia Super Corridor (MSC) project, online access remains very much an urban phenomenon. There is a clear urban-rural gap,

[1] MIMOS History, http://www.mimos.my/index.php?sub=2&ma=36, accessed March 20, 2009
[2] Household use of the Internet Survey 2008, http://www.skmm.gov.my/Admin/WhatIsNew/CCD09/HUIS2008.pdf, accessed March 20, 2009
[3] *The Star,* "Celcom's about-turn success," February 28, 2009, http://biz.thestar.com.my/news/story.asp?file=/2009/2/28/business/3367612&sec=business, accessed March 20, 2009

with more than 80 percent of internet users living in urban areas.[4] A similar gap persists in mobile-phone usage, with rural residents accounting for just 22 percent of the country's users.[5] However, according to the Malaysian Communications and Multimedia Commission (MCMC), the national mobile-phone penetration rate was 93.9 percent in 2008, much higher than the internet-penetration figure.[6] The spread of mobile-phone access, including in rural areas, has made SMS (text messaging) an increasingly important factor in the Malaysian political landscape.[7]

In recent years, the Malaysian government has been particularly aggressive in promoting broadband access, and the country is now home to more than 1.4 million broadband users.[8] Indeed, in October 2008 the Energy, Water, and Communications (EWC) Ministry threatened to revoke the WIMAX (Worldwide Interoperability for Microwave Access) licenses of companies that failed to roll out the service within the prescribed timeframe.[9] The cost of internet access is reasonable relative to the gross national income (GNI) per capita of $6,540.[10] A broadband connection package (1 megabit per second/384 kilobits per second) offered by the largest ISP in the country cost the average consumer around $25 per month in 2008.[11] Any package slower than a broadband connection is significantly cheaper. User-generated-content websites such as YouTube, social-networking sites like Facebook, and blog-hosting services including Blogspot.com and Wordpress.com are freely available.

Currently the internet falls under the immediate purview of the MCMC, a regulatory body that answers to the EWC minister. Both the MCMC and the ministry are guided by the 1998 Communication and Multimedia Act (CMA), which gives the EWC minister a wide range of licensing and other powers. Under the CMA, a license is required to own and operate a network facility. There have not been any reported denials of ISP license applications, but the licensing process could be a form of control, and the owners of major ISPs and mobile-phone service providers often have connections to the government. Of the two largest ISPs, TMnet and Jaring, the former is a subsidiary of the privatized national phone company Telekom Malaysia, and the latter is wholly owned by the Ministry of Finance. Maxis Communications, the largest mobile-phone service provider, was the founded by Ananda Krishnan, who also owns the largest satellite broadcaster and enjoys close ties to former prime minister Mahathir Mohamad. The state government in Selangor imposed a freeze on new applications for cybercafes, but it was lifted in January 2008 after 38 months. The freeze was imposed primarily due to the widespread use of cybercafes as illegal

4 Communications and Multimedia Selected Facts and Figures 2008 Q1, http://www.skmm.gov.my/facts_figures/stats/index.asp, accessed March 20, 2009

5 Handphone user survey in 2007, http://www.skmm.gov.my/facts_figures/stats/pdf/Handphone_Users_Survey_2007.pdf, accessed March 20, 2009

6 Cellular phones in Malaysia, http://www.skmm.gov.my/facts_figures/stats/ViewStatistic.asp?cc=13949228&srid=9247989, accessed March 20, 2009

7 Cellular phones in Malaysia, http://www.skmm.gov.my/facts_figures/stats/ViewStatistic.asp?cc=13949228&srid=9247989, accessed March 20, 2009

8 Number of broadband subscriptions by technology, http://www.skmm.gov.my/facts_figures/stats/ViewStatistic.asp?cc=82923074&srid=36429996, accessed March 20, 2009

9 Syarikat gagal tawar WiMax hadapi kemungkinan ditarik balik lessen, http://www.utusan.com.my/utusan/info.asp?y=2008&dt=1028&pub=utusan_malaysia&sec=Terkini&pg=bt_10.htm&arc=hive, accessed March 30, 2009

10 Country Snapshot - Malaysia, http://rru.worldbank.org/BESnapshots/Malaysia/default.aspx, accessed March 20, 2009; figure not at Purchasing Power Parity (PPP)

11 TMNet Website, http://www.streamyx.com.my/get_streamyx/get_streamyx.php?id=getstreamyx_package_standard, accessed March 20, 2009

gambling and gaming centers that operate at late hours and attract a predominantly school-age clientele, as opposed to a deliberate restriction on public access to the internet.[12]

Limits on Content

The Malaysian government does not employ any known filtering technology to actively censor internet content or limit internet communications. There are no specific laws aimed at limiting or censoring the internet, and a provision of the CMA explicitly states that nothing in the act "shall be construed as permitting the censorship of the Internet." The MSC Bill of Guarantees also promises no censorship of the internet. However, the extensive powers available to the government under older laws such as the Sedition Act, the Official Secrets Act (OSA), and the Internal Security Act (ISA) are likely to encourage self-censorship among internet users.

The government has generally upheld its promises on direct censorship, except in the case of the MCMC's decision to block the controversial website MalaysiaToday. The site, a news-aggregating portal founded by Raja Petra Kamarudin, has been very critical of the ruling party. On August 28, 2008, the MCMC ordered all major ISPs to block MalaysiaToday. Home Minister Syed Hamid Albar justified the move by citing Sections 263 and 233 of the CMA, which penalize "improper use of facilities or network services."[13] The ban was repealed by the cabinet two weeks later, but EWC Minister Shaziman Abu Mansor argued that the reversal was acceptable because there were other, "harsher" laws available, including the Internal Security Act and the Sedition Act. Along with the ban on MalaysiaToday, the MCMC also lifted bans on about 100 other websites that had previously been blocked due to pornography or financial scams. There are no other known websites being banned, filtered, or blocked by the government. However, users continue to be discouraged from expressing views related to sensitive or "red-line" issues such as Islam's official status, race, and the special rights enjoyed by *bumiputera* (ethnic Malays and other indigenous people, as opposed to ethnic Chinese and Indian minorities).

There is a vibrant blogosphere in Malaysia. Currently the dominant language of blogging is English, with Malay used to a lesser extent. This may be attributed to the nature of the user base, which consists largely of highly educated urban professionals who are more comfortable with the English language. Many civil society groups have an online presence, but in some cases their websites are not regularly updated. All mainstream news outlets have corresponding websites that mirror the print format and do not deviate from progovernment editorial policies.

Political parties have been able to use the internet to disseminate political messages and to mobilize the people. This was illustrated in the March 2008 general election, and also in the mounting of numerous public rallies and protests. Three of the country's largest telecommunications companies reportedly experienced a surge in SMS traffic during nomination day on February 24, and polling day on March 8.[14] Videos of political speeches and public protests were widely distributed on the internet through blogs and video-sharing websites. In 2006, an incident involving an anonymous video clip shot using a mobile phone—dubbed the "nude ear-squat case"—prompted an investigation by a royal commission into police operating procedures on body searches of detainees.

---

[12] *The Star*, "Abide by guideline on cyber café," January 21, 2008, http://thestar.com.my/metro/story.asp?file=/2008/1/21/central/20059112&sec=central, accessed March 20, 2009

[13] *The Star*, "Syed Hamid tells why Malaysia Today was blocked," August 29, 2008, http://thestar.com.my/news/story.asp?file=/2008/8/29/nation/22194389&sec=nation, accessed March 20, 2009

[14] *The Star*, "Surge in SMS traffic on election day," March 30, 2008, http://thestar.com.my/news/story.asp?file=/2008/3/30/focus/20788837&sec=focus, accessed March 20, 2009

Violations of Users' Rights

Although the current government has been active in trying to eliminate infrastructural and economic obstacles to internet access and does not filter online content, there have been major violations of user rights. Certain provisions in the MSC Bill of Guarantees[15] and the CMA[16] offer some protections, but the authorities have been able to circumvent them by making arbitrary arrests under preexisting laws. This is part of a larger phenomenon in which the laws governing freedom of expression in more traditional media have begun to spill over into cyberspace.

Defamation charges have been filed against bloggers in Malaysia, most notably Ahirudin Attan and Jeff Ooi in January 2007. They were targeted by the progovernment media conglomerate NSTP Group, prompting the establishment of the National Alliance of Bloggers (All-Blogs). The case is currently in a state of limbo, with neither side actively pursuing it. More recently, blogger Raja Petra Kamarudin was served with criminal defamation charges by two military officers who objected to being implicated in the politically charged murder of a Mongolian model.[17] In May 2008, he was arrested under the Sedition Act for an article linking Deputy Prime Minister Najib Abdul Razak and his wife to the murder.[18] Raja Petra was then arrested in September 2008 under the ISA, which allows indefinite detention without trial. He was released in November after the High Court ruled that the detention was unconstitutional. Raja Petra had previously been arrested under the ISA in 2001, and he was interrogated by the police for eight hours in July 2007 for allegedly insulting the monarchy and Islam on his blog.[19]

In July 2007, the police arrested blogger Nathaniel Tan under the OSA.[20] Tan, an assistant to opposition leader Anwar Ibrahim at the time, was held responsible for the comments posted on his blog site. He was remanded for four days and subsequently released. Yet another blogger, Syed Azidi Syed Aziz, was arrested under the Sedition Act in September 2008 for inciting his readers to fly the Malaysian flag upside down.[21]

In August 2007, a parody of the national anthem on the video-sharing website YouTube was posted by university student and musician Wee Meng Chee, also known as NameWee. In response, Mohammed Nazri Abdul Aziz, then a minister in the Prime Minister's Department, called for actions to be taken "against YouTube and bloggers for posting images and content that overstepped the boundaries on sensitive issues."[22] Wee, who was studying in Taiwan at the time, apologized for the controversy he had caused.

---

15 MSC Malaysia 10-Point Bill of Guarantees, http://www.mscmalaysia.my/topic/MSC+Malaysia+Bill+of+Guarantees, accessed March 20, 2009

16 Communication and Multimedia Act 1998, http://www.skmm.gov.my/mcmc/the_law/NewAct/Act%20588/Act%20588/a0588.htm, accessed March 20, 2009

17 "Blogger Raja Petra Sued By Two Army Personnel Implicated In His Statutory Declaration," Bernama, July 22, 2008, http://www.bernama.com.my/bernama/v3/news.php?id=347708, accessed March 20, 2009

18 *The Sun Daily,* "Blogger charged with sedition," May 6, 2008, http://www.thesundaily.com/article.cfm?id=22064, accessed March 20, 2009

19 *The Star,* "Webmaster Raja Petra questioned for 8hrs," July 25, 2007, http://thestar.com.my/news/story.asp?file=/2007/7/25/nation/20070725205852&sec=nation, accessed March 20, 2009

20 *The Star*, "Nathaniel Tan remanded for four days under OSA," July 14, 2007, http://thestar.com.my/news/story.asp?file=/2007/7/14/nation/20070714182404&sec=nation, accessed March 20, 2009

21 *The Star,* "Blogger Sheih Kickdefella under 24-hour remand," September 19, 2008, http://thestar.com.my/news/story.asp?file=/2008/9/19/courts/2064905&sec=courts, accessed March 20, 2009

22 *The Sun Daily,* "Who is sorry now?" August 16, 2007, http://www.thesundaily.com/article.cfm?id=19009, accessed March 20, 2009

The EWC minister reportedly said in September 2008 that the MCMC had formed a committee comprised of the police, officials from the attorney general's office, and representatives of the Home Ministry to monitor websites and blogs.[23] It is unclear to what extent these monitoring efforts have been implemented. There has been no known effort at surveillance of mobile-phone usage. Beginning in 2007, all mobile users, including roughly 18 million prepaid users, were required to register as part of an effort to decrease rumor-mongering activities via SMS.[24] It would appear, however, that such registration measures have been weakly enforced. Users in cybercafes are not required to register.

While bloggers, online journalists, and other ICT users are subject to arbitrary arrest, they generally do not face extralegal intimidation or physical violence. Still, some bloggers have reported receiving threatening messages from anonymous users. Of the bloggers arrested between 2006 and 2008, none were reported to have been abused physically while in custody.

[23] *The Star,* "Existing laws to deal with websites that cause unease," September 12, 2008, http://www.thestar.com.my/news/story.asp?file=/2008/9/12/nation/2010044&sec=nation, accessed March 20, 2009

[24] "Dec 15 Registration Deadline Stays: MCMC," August 18, 2006, http://www.bernama.com.my/bernama/v3/news.php?id=214811, accessed March 20, 2009

Russia

Status: Partly Free

Obstacles to Access: **11** (0–25)
Limits on Content: **17** (0–35)
Violations of User Rights: **23** (0–40)
Total Score: **51** (0–100)

Population: 141.7 million
Internet Users/Penetration 2006: 25.7 million / 18 percent
Internet Users/Penetration 2008: 29.8 million / 21 percent
Mobile Phone Users/Penetration 2006: 151 million
Mobile Phone Users/Penetration 2008: 187 million
Freedom of the Press (2008) Score/Status: 78 / Not Free
Digital Opportunity Index (2006) Ranking: 51 out of 181
GNI Per Capita (PPP): $14,400
Web 2.0 Applications Blocked: No
Political Content Systematically Filtered: No
Bloggers/Online Journalists Arrested: Yes

Introduction

Since the internet was first launched in Russia in 1988, the country has made significant gains in the expansion of its information infrastructure. Most Russians access the internet from their homes (71 percent of users) and workplaces (41 percent), whereas only about 6 percent use cybercafés. [1] Internet access via mobile telephones and similar devices has gained popularity since 2006, and 10 percent of users currently report using this method. [2] The web is used primarily to check e-mail and for entertainment purposes, and only secondarily to read news reports and blogs.

After the elimination of independent television channels in 2000–01 and the tightening of press regulations, the internet became the last relatively uncensored platform for public debate and the expression of political opinions. There have not been any significant cases of technical blocking or filtering, but the authorities have increasingly engaged in intentional content removal. Internet freedom has corroded significantly in recent years, and this trend is borne out by the statistics: one internet activist killed, seven criminal cases launched against bloggers, one blogger badly beaten, and ten oppositional blogs attacked by hackers. The legal environment is threatened by a number of new legislative initiatives, and some have even proposed building a massive filtering and censorship apparatus in the mold of China's infamous "Great Firewall."

Obstacles to Access

Internet and mobile-phone penetration in Russia continues to grow, and the government largely supports the dissemination of these technologies. The number of internet users jumped from 1.5 million in 1999 to 29.8 million in 2008,[3] although this still gives Russia a much lower penetration rate than that in Western Europe, and more than half of Russia's users are concentrated in the two largest cities.[4] Mobile use expanded even more rapidly, rising from a few million subscribers in the late 1990s to 187 million—about 35 million more than the country's actual population—in 2007.[5] The Russian mobile market in 2006 became the third largest in the world by subscribers and

1 http://bd.fom.ru/report/cat/smi/smi_int/int0803, accessed March 20, 2009.
2 http://www.gfk.ru/Go/View?id=338, accessed March 20, 2009.
3 ITU, http://www.itu.int/ITU-D/icteye/default.aspx
4 http://trends.spylog.ru/global-statistic-city/, accessed March 20, 2009.
5 ITU, http://www.itu.int/ITU-D/icteye/default.aspx

revenue, after China and the United States. A massive campaign to connect all Russian schools to the internet began in 2002. While the majority of the schools were connected by the end of 2008, the speed of the link is unacceptably slow at 128 kilobits per second; this connection is shared by a given school's entire stock of 30 to 60 computers. [6] Although dial-up internet access costs roughly the same across the country, the prices for broadband access in the majority of Russia's regions are four times higher than in Moscow.[7] There are infrastructural limitations to internet access, but the government does not widely block access to the web or to specific web-based applications. The YouTube video-sharing platform, the social-networking site Facebook, and various international blog-hosting services are freely available.

Nearly 75 percent of Russian users still have dial-up. [8] The broadband market, which rose from 3.6 million users in 2006 to 8.3 million in 2008, is relatively liberalized. The state-owned provider SvyazInvest accounts for only 27.8 percent of broadband users, with the rest served by private companies. Many of those are regional companies affiliated with large national firms. As at the federal level, regional ownership usually depends on political connections and the tacit approval of regional authorities. Although this situation is not the direct result of legal or economic obstacles, it nonetheless reflects an element of corruption that is widespread in the telecommunications sector as well as other parts of the Russian economy.

Three leading operators—MTS, Vimpelcom, and MegaFon—hold 85 percent of the mobile-phone market.[9] While formally independent, each of these firms has indirect ties to the government. According to independent analyst Vadim Gorshkov, MegaFon is connected with former minister of telecommunications Leonid Reyman, and MTS is linked to the Moscow regional leadership.[10] The information and communications technology (ICT) sector is regulated by the Federal Service for the Supervision of Communications and Mass Communications, whose director is appointed by the prime minister. The appointment process is not transparent. Boris Boyarskov, the head of the service for four years until his replacement by a subordinate in December 2008, reportedly served in the KGB during the Soviet era.[11] There are no special restrictions on opening cybercafés or starting internet service provider (ISP) businesses, although unfair competition and other such obstacles are not unusual in Russia.

Limits on Content

Legal controls on the internet were first proposed in 1996 by leftist members of parliament, though no action was taken at the time. Since then, however, the authorities have pursued various methods of censorship. In October 2008, a leading information-technology company official, Valentin Makarov, proposed building a Russian version of China's so-called Great Firewall within the next 10 years.[12] Until such a nationwide filtering apparatus is created, website operators and users can evade state interference fairly easily by utilizing foreign hosting services.

---

6 Industry experts' opinion.

7 Based on the comparative research of the ISP prices: http://eburg.nag.ru/, accessed March 20, 2009.

8 http://rumetrika.rambler.ru/publ/article_show.html?article=3542, accessed March 20, 2009.

9 "Russian Telecom Sector - Dynamic Growth in 2006," Ezine @rticles, http://ezinearticles.com/?Russian-Telecom-Sector---Dynamic-Growth-in-2006&id=552086, accessed March 20, 2009.

10 http://www.compromat.ru/main/reiman/megafon.htm, and http://www.compromat.ru/main/luzhkov/sistema1.htm, accessed March 20, 2009.

11 RFERL Newsline, April 21, 2004, http://www.hri.org/news/balkans/rferl/2004/04-04-21.rferl.html, accessed March 20, 2009 and "Kremlin appears to be rattled by unrest," *St. Petersburg Times,* December 16, 2008, http://www.sptimes.ru/index.php?action_id=2&story_id=27850&highlight=boyarskov, accessed March 25, 2009.

12 http://www.cnews.ru/news/top/index.shtml?2008/10/24/324624, accessed March 20, 2009.

There has been only one well documented case of systematic blocking or filtering by ISPs, and it was later downplayed. The website affected, Kompromat.ru, was blocked by several providers in the run-up to the 2008 presidential election.[13] After the action became public, and the election was over, the filter was removed. However, the practice of exerting pressure by telephone is quite widespread. It is carried out not only by security agencies but also by Kremlin and regional administration officials, who call owners, shareholders, and anyone else in a position to remove unwanted material and ensure that the problem does not come up again. After receiving such calls, managers and editors are more likely to practice self-censorship. The director of leading hosting company Masterhost, Aleksandr Ovchinnikov, admitted that his company gets about 100 requests daily from the authorities to black out "inconvenient"—usually nationalistic or antigovernment—websites.[14] Commenting on the Kompromat case, Ovchinnikov said the order to block the site was made "with a phone call." A similar practice was used in the case of the website of the newspaper *Vyatskii Nablyudatel*, which was closed in April 2008 at the request of the Kirov regional police due to a forum comment criticizing the regional leadership. After the incident, the newspaper website moved to a foreign host to protect itself from further government threats.[15]

There is little evidence of intentional and illegal removal of blog posts. On the Livejournal blogging platform, for instance, posts have been removed only if they violated privacy rights (by including personal address details or other private data) or promoted terrorism. However, illegal content removals do occur. In March 2008, the website islam.boom.ru was closed because the prosecutor's office said that it was spreading extremism.[16] In October 2008, hosting service HostZona.ru closed the website Putin-loh.ru ("Putin is a dumbass").[17] The host's director explained that the content of the website insulted the prime minister and it was his civic duty to close it down.

When the web was not such a popular phenomenon, the Kremlin was able to exert its influence with rather limited means, for example by forum trolling (in internet slang, a troll is someone who posts controversial, inflammatory, irrelevant, or off-topic messages in an online community) and establishing propaganda websites.[18] The so-called Brigade, a pro-Kremlin group formed by paid bloggers and volunteers, is still active, but its influence declined as other users identified its members and began to ban trolls.

The situation started to change after the "color revolutions" in three former Soviet countries in 2003–05, when information technology played a significant role in mobilizing large numbers of people for political protests. In November 2007, Deputy Prosecutor General Ivan Sydoruk proposed increasing government control over the internet.[19] The ruling United Russia party presented legislation in February 2008 that would require internet sites with over 1,000 visitors per day to register with the authorities, making them equivalent to print media with circulations of 1,000 or more copies, but the measure was not enacted.[20] Many Russians view the internet as a proper sphere for governmental control. According to a Levada-Center poll taken in December 2006, some 22 percent would "absolutely agree" and another 22 percent would "rather agree" with the statement "It's time to bring order to the internet."[21] However, the Kremlin is not unified on the issue. There have been constant tensions between social conservatives who express aspirations to

[13] http://habrahabr.ru/blogs/telecom/20677/, accessed March 20, 2009.
[14] http://www.nr2.ru/moskow/169361.html, accessed March 20, 2009.
[15] http://www.svobodanews.ru/Article/2008/04/23/20080423132141247.html, accessed March 20, 2009.
[16] http://www.webplanet.ru/news/law/2008/03/07/islamboom.html, accessed March 20, 2009.
[17] http://www.kavkazcenter.com/russ/content/2008/10/09/61480.shtml, accessed March 20, 2009.
[18] More on that topic here: http://ds.ru/ss1.htm
[19] http://www.kommersant.ru/doc.aspx?docsid=776912, accessed March 20, 2009.
[20] http://www.newsru.com/russia/11feb2008/websmi.html, accessed March 20, 2009.
[21] http://www.levada.ru/press/2008071701.html, accessed March 20, 2009.

overtly control the internet (the United Russia party, together with the influential "siloviki" faction, the Federal Security Service [FSB], and the prosectutor's office) and centrists (Prime Minister Vladimir Putin, President Dmitri Medvedev, and current and former ministers of communications Igor Shchegolev and Leonid Reyman) who do not want to damage their international reputations with censorship scandals and prefer more sophisticated tools to control internet content.

Russia's vibrant blogosphere includes over 3.8 million blogs.[22] Approximately 80 percent of Russian-language bloggers live inside the country with the remaining 20 percent living outside in the large Russian diaspora.[23] President Medvedev started a video blog in October 2007, and three regional governors followed suit.[24] Unfortunately, blogs do not have a major influence on political life. This is due less to the apathy of Russian web users than to the government's success in preventing online activism from spreading to the streets or reaching wider media audiences. Almost all large non-governmental organizations (NGOs) (based in Moscow and Saint Petersburg) have their own websites, but those based in the regions are less likely to have a presence online. Non-Russian-speaking ethnic groups are underrepresented on the web. There is little discussion of the Chechnya issue, as opposed to the leadership of Chechen president Ramzan Kadyrov. During the Russian-Georgian conflict of August 2008, the Russian blogosphere, even its liberal elements, generally supported the Russian invasion.

Livejournal is the most popular blogging platform, accounting for 45 to 50 percent of all Russian-language blogs. This may be due to its adoption by a group of the Russian internet elite (Anton Nossik and Yuri Zasurski, among others). Other factors include the site's "friendship" mechanism and the relative simplicity of the interface.

The Kremlin allegedly started to influence the blogosphere in 1999–2000 through just one organization, the Foundation on Effective Politics, led by Gleb Pavlovski.[25] In 2006–08, the Russian internet experienced a proliferation of Kremlin-affiliated "content providers" that were essentially propaganda sites.[26] Among the new net-propagandists were Konstantin Rykov and his New Media Stars,[27] Vadim Gorshenin of Pravda.ru,[28] and Aleksey Chesnakov of the Center for Political Conjuncture Research. Each of these media managers, according to prominent journalist Oleg Kashin, has a liaison on the president's staff. The emergence of competing propagandist websites led to the establishment of a vast network of online propaganda that collectively dominates search results, among other effects.[29]

If an opposition or grassroots organization starts its own internet platform, Kremlin-related groups will launch several that are similar in form, if not in content. These sites create confusion among users by adopting similar imagery, slogans, and names. Meanwhile, bloggers who report on regional protests or some other sensitive incident are swamped by other blogs that give an opposite account, sometimes using sophisticated language but also resorting to obscenity to discourage debate.

The topics targeted with such tactics vary from region to region but often include political opposition, dissidents like Mikhail Khodorkovsky, murdered journalists, jobs and working conditions, and cases of international conflict or rivalry (with countries such as Estonia, Georgia,

[22] http://download.yandex.ru/company/yandex_on_blogosphere_spring_2008.pdf, accessed March 20, 2009.
[23] http://download.yandex.ru/company/yandex_on_blogosphere_spring_2008.pdf, accessed March 27, 2009.
[24] http://blog.kremlin.ru/, accessed March 20, 2009.
[25] http://ds.ru/ss1.htm accessed March 27, 2009
[26] http://www.openspace.ru/media/net/details/7946/page1/, accessed March 20, 2009.
[27] Rykov's projects include: vzglyad.ru, Russia.ru, chaskor.ru, litprom.ru; see also: http://avmalgin.livejournal.com/529896.html, accessed March 27, 2009
[28] Gorshenin's projects include: yoki.ru, politonline.ru, electorat.info
[29] http://www.vremya.ru/2008/152/4/210951.html, accessed March 27, 2009

and Ukraine, but also over U.S. and European foreign policies). The issue of spontaneous protests triggered by the economic crisis appears to be a growing concern.

The most successful civic action coordinated with the help of online forums and blogs was the movement against the restriction of right-hand-drive automobiles, which are imported from Japan and used widely in the Far East. Beginning in 2005, the organization Freedom of Choice (Svoboda Vybora) used forums to organize political action in different cities in Siberia.[30] In addition to thwarting government attempts to discontinue the use of right-hand-drive cars, the group has taken up other issues important to motorists, including road quality, taxes, insurance rates, and special driving rules for senior government officials.

There is little information on the use of SMS, or text messaging, in political agitation. However, presidential staff used SMS in mobilizing people to participate in national elections in 2007.[31] The same practice was used in several regional election campaigns.[32] Certain mobile operators like Vimpelcom have stated that they prohibit political agitation through SMS. The use of political SMS messages is linked to other problems, including loose laws on commercial advertisements via SMS.[33]

As social-networking sites and blogger platforms have grown in importance, they have caught the attention not only of the Russian government but also of Russian business magnates, or oligarchs. Since they are eager to maintain good relations with the Kremlin, oligarchs are likely to resort to various nontransparent practices to ensure that their web services are free of objectionable material or activity. In December 2007, a day after the parliamentary elections, Livejournal was bought by the oligarch Aleksandr Mamut.[34] Some journalists accused the new owners of leaking "closed" and "friends-only" entries to the police and the FSB. In December 2007, the creator of the most popular social-networking site, Odnoklassniki, publicly announced that his service refused to cooperate with the FSB.[35] Although the veracity of his statement remains uncertain, it suggests that the FSB has pursued such cooperation. In June 2008, the Kremlin-affiliated oligarch Alisher Usmanov bought a 50 percent stake in Livejournal from Mamut.[36] In July, Usmanov announced his purchase of significant stakes in Odnoklassniki and another social-networking site, Vkontakte.[37]

Violations of Users' Rights

Since 2006, conditions for user rights in Russia have significantly worsened. Bloggers have become subject not only to hacker attacks but also to physical violence and legal prosecution. Although the constitution grants the right of free speech, there are no special laws protecting online modes of expression, and even constitutional guarantees are routinely violated. Online journalists do not possess the same rights as regular journalists unless they register their websites as mass media. Recent police practice has been to target online expression using Article 282 of the criminal code, which restricts extremism. The term is vaguely defined and includes xenophobia and incitement of hatred toward a social group.

---

30 http://www.19may.ru/, accessed March 20, 2009.
31 http://www.kommersant.ru/doc.aspx?DocsID=830972, accessed March 20, 2009.
32 http://www.cnews.ru/news/top/index.shtml?2007/03/19/240836 and http://www.htcom.ru/news-mobile/newsd-19789/ and http://www.expert.ru/news/2007/02/26/sms_golosovanie/, accessed March 20, 2009.
33 http://e-moe.com.ua/node/786, accessed March 20, 2009.
34 http://www.kommersant.ru/doc.aspx?DocsID=831892, accessed March 20, 2009.
35 http://hitech.newsru.com/article/21dec2007/fsb , and http://www.kp.ru/daily/24022/90256/, accessed March 20, 2009.
36 http://www.dengi.ua/news/38264.html, accessed March 20, 2009.
37 http://www.kp.ru/online/news/117169/, accessed March 20, 2009.

Following the 2007 parliamentary elections, the government launched at least seven criminal cases against blog and forum writers. In the best-known case, 23-year-old blogger Savva Terentyev was convicted in July 2008 of denigrating the human dignity of a social group—the police—and sentenced to one year of probation.

The government's technical capabilities in monitoring online activity have risen drastically in recent years. Since 2000, all ISPs have been obliged to install the "system for operational investigative measures,"[38] or SORM-2, which gives the FSB and police access to internet traffic. The system is analogous to the Carnivore/DCS1000 software implemented by the U.S. Federal Bureau of Investigation (FBI), and operates as a packet-sniffer which can analyze and log data passing over a digital network.[39] However, no known cases of SORM-2 use have been reported. Legislation approved in April 2007 allows government services to intercept data traffic without a warrant,[40] and in August 2008, the FSB announced the creation of a new portal to monitor the Russian internet and mass media. Little detailed information has been released on how the portal works, although the main aim of the project is the monitoring of public opinion.

Hacker attacks on opposition bloggers became a mass phenomenon in the summer of 2007, in the run-up to the parliamentary elections. Ten popular bloggers were targeted by a group of hackers sponsored by Kremlin-affiliated political operatives. The blogs were ravaged and defaced. DDoS (Distributed Denial of Service) attacks became another powerful instrument of the Kremlin's hidden influence. In May 2007, during a major public and diplomatic row with Estonia over the fate of a Soviet war memorial in the Estonian capital, numerous Estonian government and other websites were attacked, and few Kremlin-based internet-protocol addresses were spotted.[41] A similar tactic was used during the Russian-Georgian conflict of 2008, although the Georgian side also used DDoS attacks, combined with ISP filtering of the ".ru" country code.[42] During the 2007 electoral campaign, the websites of three parties—the Union of Rightist Forces (SPS),[43] Yabloko,[44] and the Liberal Democratic Party of Russia (LDPR)[45]—were attacked.

When there are no grounds for a criminal case, physical violence has been used against bloggers and online commentators. Citizen reporter and blogger Grigorii Belonuchkin was beaten after filing a voting-fraud lawsuit against a local electoral commission in April 2008.[46] Well-known political activist Magomed Yevloyev, creator of the Ingushetia.ru website, was killed by personal security agents of Murat Zyazikov, the president of the Russian republic of Ingushetia, after being detained at the local airport.[47] Zyazikov was dismissed two months later, but no criminal case was launched against him or his security personnel.

---

[38] http://www.iksmedia.ru/topics/analytical/effort/261924.html?__pv=1, more info on the SORM, http://www.sorm-li.ru/sorm2.html, accessed March 20, 2009.
[39] http://www.protei.ru/company/pdf/publications/2007/2007-003.pdf, accessed March 20, 2009.
[40] http://www.consultant.ru/online/base/?req=doc;base=LAW;n=83144, accessed December 2008.
[41] http://dw-club.com/dw/article/0,,2542160,00.html, accessed March 20, 2009.
[42] http://www.kommersant.ru/doc.aspx?docsid=1080963, accessed March 20, 2009.
[43] http://www.kommersant.ru/doc-rss.aspx?DocsID=826114, accessed March 20, 2009.
[44] http://www.grani.ru/Politics/Russia/m.139854.html, accessed March 20, 2009.
[45] http://www.kommersant.ru/doc.aspx?DocsID=796719, accessed March 20, 2009.
[46] http://www.golos.org/a1376.html, accessed March 20, 2009.
[47] http://www.kommersant.ru/doc.aspx?DocsID=1018915, accessed March 20, 2009.

South Africa

Status: Free

Obstacles to Access: **6** (0–25)
Limits on Content: **7** (0–35)
Violations of User Rights: **8**(0–40)
Total Score: **21** (0–100)

Population: 48.8 million
Internet Users/Penetration 2006: 3.7 million / 8 percent
Internet Users/Penetration 2008: 4 million / 8 percent
(Note: relates to access via computer; an estimated 9.5 million / 19 percent accessed via mobile phone)
Mobile Phone Users/Penetration 2006: 39.7 million
Mobile Phone Users/Penetration 2008: 45 million
Freedom of the Press (2008) Score/Status: 28 / Free
Digital Opportunity Index (2006) Ranking: 86 out of 181
GNI Per Capita (PPP): $9,600
Web 2.0 Applications Blocked: No
Political Content Systematically Filtered: No
Bloggers/Online Journalists Arrested: No

Introduction

There is a high level of digital media freedom in South Africa. Political content is not censored, and bloggers are not prosecuted for online activities. The country is in the exceptional position of having more people accessing the internet from their mobile telephones than from their computers. Nevertheless, the majority of the population is unable to benefit from internet access due to high costs and the fact that most content is in English, an obstacle for those who speak only local dialects. Despite several positive court rulings, there are also increasing concerns that precedents established by defamation cases involving traditional media may be used to limit free speech online, especially in forums like the social-networking site Facebook.

Obstacles to Access

Access to the internet has steadily improved in South Africa despite the obstacles that remain. It is estimated that about 8 percent of the population – 4 million people – has access, one of the highest rates in Sub-Saharan Africa. However prices are still beyond the reach of the majority of the population.[1] Most of those with access, especially broadband access, are concentrated in urban areas. After years of stifled competition, the market is slowly opening up, and it is expected that costs will drop with the arrival of the Seacom undersea fiber-optic cable in 2009 and the increasing use of updated mobile-phone technology. Telkom SA, a partly stated-owned company, retains a near monopoly in providing broadband access via ADSL, though the recent licensing of a second national operator, Neotel, should increase competition.

A number of companies offer broadband alternatives via mobile phones, including Iburst, Cell C, MTN, and Vodacom. South Africa is thus in an unusual position in that mobile broadband is cheaper than the fixed-line alternative, which remains extremely expensive. As of 2008, 9.5 million South Africans accessed the internet via mobile phones, slightly more than double the number of

[1] ITU, http://www.itu.int/ITU-D/icteye/Default.aspx, Accessed on 3/27/2009

those who connected via computers.[2] This gap is expected to increase given the extensive mobile-phone penetration and the fact that South Africa's mobile internet access is among the cheapest in the world. The total number of mobile-phone subscribers is estimated to be 45 million.[3] The government has not imposed restrictions on internet access, and there have been no reports that the authorities use control over internet infrastructure to limit connectivity. Individuals and groups can engage in peaceful expression of views via the internet using e-mail, instant messaging, chat rooms, and blogs. The video-sharing site YouTube, Facebook, and international blog-hosting services are freely available.

In August 2008, a court ruled that value-added network service (VANS) providers can self-provide, ending a long battle by the industry against the Department of Communications. It is expected that this will lead to more competition in the internet-access sector. In addition, compulsory partial ownership of communications companies by black shareholders, as part of the government's Black Economic Empowerment policy, is expected to further advance diversification in the ownership of internet-service providers (ISPs).

The autonomy of the Independent Communications Authority of South Africa (ICASA) is protected by law, and there have been no reports of government interference with its decisions. It has been accused of favoring Telkom SA, but in at least one instance it defied the minister of communications on a regulatory issue and was subsequently supported by a court ruling. Access providers and other internet-related groups are self-organized and quite active in lobbying the government for better regulations.

Limits on Content

There have been no reports of state censorship of internet content, with the exception of pornography. In September 2006, the government notified sites hosted in South Africa that they must cease publication of pornography by the end of that year or face criminal action under the Film and Publications Act of 1996. The vast majority of pornographic sites have since complied and removed the offending content, but some remains. A revised version of the Film and Publications Act was recently sent back to Parliament by the president. There is some concern that the law could be used to censor other kinds of online content, though this has yet to happen.[4]

The government does not restrict material on contentious topics such as corruption or human rights. Self-censorship among private individuals and journalists does not appear to be widespread, although employees at state-run media may be an exception. Online expression in general seems to be more open than other forms of communication.

Citizens are able to access a wide range of viewpoints, and there are no government efforts to limit discussion. Online content, however, does not match the diverse interests within society, especially with respect to race and local languages. There are a number of political and consumer-activist websites, though the internet is not yet a key space for social or political mobilization.

The South African blogosphere has been highly active in promotion of AIDS awareness and the discussion of environmental issues, in addition to more general political coverage. Mobile phones are being used for political organization, especially during recent developments, like the

[2] "Mobile surpasses traditional web in South Africa", *Matthew Buckland*, November 19, 2008, www.matthewbuckland.com/?p=573, Accessed on 3/27/2009
[3] ITU, http://www.itu.int/ITU-D/icteye/Default.aspx Accessed on 3/27/2009
[4] "Bloggers battle film bill," *New Media Lab*, May 8, 2007, http://nml.ru.ac.za/blog/jude/2007/05/08/bloggers-battle-film-bill.html, Accessed on 3/27/2009

establishment of the new political party COPE, a breakaway faction of the African National Congress that has ruled South Africa since the early 1990s.

Print outlets, television, and radio continue to be the main sources of news and information for most South Africans, but there are increasing efforts to extend mainstream news to online platforms, for example by the *Times* and *Mail & Guardian* newspapers, which operate affiliated websites.

Violations of Users' Rights

The constitution guarantees "freedom of the press and other media; freedom to receive or impart information or ideas; freedom of artistic creativity; and academic freedom and freedom of scientific research." However, it also includes constraints, and freedom does not extend to "propaganda for war; incitement of imminent violence; or advocacy of hatred that is based on race, ethnicity, gender, or religion and that constitutes incitement to cause harm."[5] The judiciary in South Africa is independent and has issued at least one ruling protecting freedom of expression online.

Libel is not a criminal offense, but civil laws have been applied to online content. In a recent case, Natasha Tsichlas, the manager of a South African soccer team, sued Touch Line Media for anonymous defamatory posts directed at her on the company's website, Kick Off. However, the judge found that freedom of speech on the internet would be significantly curtailed if the hosts of discussion boards were required to regulate material posted on their sites by outside parties.[6]

There have been no reports that the government monitors e-mail or internet chat rooms. Recent legislation potentially allows for extensive monitoring, but this has not yet been implemented. The Regulation of Interception of Communications and Provision of Communication-Related Information Act of 2002 (RICA) requires ISPs to retain customer data for an undetermined period of time, and bans any internet system that cannot be monitored. In addition, the Electronic Communications and Transactions Act of 2002 (ECTA) created a legion of inspectors trained to "inspect and confiscate computers, determine whether individuals have met the relevant registration provisions as well as search the Internet for evidence of 'criminal actions.'"[7] There have been no reports to date that these requirements have actually been enforced. Mobile subscribers with postpaid accounts are required to provide extensive personal information to service providers, and the data is then made available to the government. An identification number is legally required for any SIM-card purchase, although this law appears to be enforced unevenly.

The ECTA also requires ISPs to respond to and implement a "Take-Down Notice" regarding illegal content (such as child pornography, material that could be defamatory without justification, or a copyright violation). The law states that ISPs "do not have an obligation to monitor," exempting them from liability if proscribed content is found on their service but taken down once a notice is received. However, this exemption only applies if the ISPs are members of a recognized representative organization. Five years have passed since the ECTA was incorporated into South African law, but the government has so far failed to recognize any such organization. RICA provides for an "interception direction" that obliges ISPs to send the communications in question to an interception center. However, the law requires judicial oversight and includes

[5] The Constitution of the Republic of South Africa, May 8, 1996: Bill of Rights: Chapter 2, Section 16.
[6] "Tsichlas v. Touch Line Media," *The University of Pretoria*, http://www.up.ac.za/academic/law/docs/RVD110_111June_2004.doc ,Accessed December 2008
[7] "Internet Censorship Report 2003: South Africa," *APC Africa ICT Policy Monitor*, November 10, 2004, http://africa.rights.apc.org/index.shtml?apc=s21817e_1&x=28050, Accessed on 3/27/2009

guidelines for judges to establish whether the interception is justified in terms of proportionality and narrowly defined standards.

Reports indicate that the government conducts some surveillance of SMS (text messaging) and mobile-phone conversations. The National Communications Centre (NCC) reportedly has the technical capabilities and staffing to monitor both SMS and voice traffic originating outside South Africa.[8] Calls from foreign countries to recipients in South Africa can allegedly be monitored for certain keywords; the NCC then intercepts and records flagged conversations. While most interceptions involve reasonable national security concerns, such as terrorism or assassination plots, the system allows the NCC to record South African citizens' conversations without a warrant.[9]

There have been no reports of extralegal intimidation targeting online journalists, bloggers, or other digital-technology users by state authorities or any other actor.

[8] "Every call you take, they'll be watching you," *IOL*, August 24, 2008, http://www.iol.co.za/index.php?set_id=1&click_id=13&art_id=vn20080824105146872C312228, Accessed on 3/27/2009

[9] ibid.

Tunisia

Status: Not Free

Obstacles to Access: **20** (0–25)
Limits on Content: **27** (0–35)
Violations of User Rights: **31** (0–40)
Total Score: **78** (0–100)

Population: 10.4 million
Internet Users/Penetration 2006: 953 thousand / 9 percent
Internet Users/Penetration 2008: 1.7 million / 17 percent
Mobile Phone Users/Penetration 2006: 7.3 million
Mobile Phone Users/Penetration 2008: 7.9 million
Freedom of the Press (2008) Score/Status: 81 / Not Free
Digital Opportunity Index (2006) Ranking: 86
GNI Per Capita (PPP): $7,100
Web 2.0 Applications Blocked: Yes
Political Content Systematically Filtered: Yes
Bloggers/Online Journalists Arrested: Yes

Introduction

The internet was first launched for public use in Tunisia in November 1996, and broadband connections were first made available in November 2005. Since traditional media are censored and tightly controlled by the government, the internet has been used as a relatively free and uncensored means of airing political and social opinions, and as an alternative field for public debates on serious political issues. This uncontrolled freedom of expression has led to the creation of an extensive censorship and filtering system.

Obstacles to Access

Internet usage in Tunisia has grown rapidly in the past few years, even as access remains restricted. The government claims that there are 2.8 million internet users in the country, for a penetration rate of nearly 27 percent[1]—the ITU places this figure closer to 1.7 million users or a 17 percent penetration rate[2]—and some 8.6 million mobile-phone subscribers.[3] However, access to information and communication technologies (ICTs) remains difficult for most Tunisians due to high costs and an underdeveloped infrastructure. Tunisia has only one land-line service provider, Tunisie Telecom, and every internet subscriber is forced to first buy a land-line telephone package that includes Tunisie Telecom internet service. Prices for Tunisie Telecom vary from 15 dinars (US$12) for a connection speed of 128 to 256 kilobits per second, to 50 dinars (US$35) for a speed of 512 kilobits to 2 megabits per second. Prices for subscriptions to other internet service providers (ISPs) are similar, although they range as high as 70 dinars for the higher connection speed. Mobile internet access is rarely used, since mobile-phone companies purchase internet access from existing ISPs and the cost remains beyond the reach of most Tunisians. Although there are no legal limits on the data capacity that ISPs supply, the bandwidth remains very low and connectivity is highly dependent upon physical proximity to the existing infrastructure.

During the past few years the government has attempted to increase access to ICTs by rebuilding infrastructure to improve connectivity, encouraging "Free Internet" programs that allow internet access for the cost of an ordinary telephone call, and promoting competition among ISPs to

[1] http://www.ati.tn/fr/index.php?id=90&rub=27, accessed December 2008
[2] International Telecommunications Union, http://www.itu.int/ICT-D/icteye/default.aspx
[3] http://www.infocom.tn/index.php?id=264, accessed on March 23, 2009

lower prices. In 2004, the government set up an initiative to encourage widespread computer use by removing customs fees and creating the Family PC concept, according to which each family should own a personal computer. Authorities set a price ceiling for computer hardware and established programs offering loans at low interest rates for families to purchase the necessary equipment. The program also provided an internet subscription with every computer sold. Unfortunately, the project did not achieve the intended results because computer prices remained prohibitively high—about 700 dinars, or three times the minimum monthly salary—even with the government incentives. Although many people are unable to connect at home, the government claims that universities, research centers, laboratories, and high schools have a 100 percent connectivity rate, and that primary schools are 70 percent connected.[4] Most Tunisian users access the internet through cybercafes known as Publinets. According to government statistics there are currently 204 Publinets across the country.[5] Yet even this method of access remains prohibitively expensive for most people, and the number of Publinets has fallen steadily over the past few years.

Tunisians enjoy access to various internet services and applications such as free blog-hosting websites. However, the private internet connections of some journalists and political bloggers are often cut due to "technical problems," or their speed is reduced to hamper their ability to view sites and post information. Furthermore, some applications like the video-sharing sites Dailymotion and YouTube have been systematically blocked by the government.[6] Systems such as Voice over Internet Protocol (VoIP) that provide PC to phone calls are prohibited, but applications like Skype and Google Talk, which also provide PC to PC calls, are accessible. The social-networking site Facebook was blocked in August 2008, and although the move was reversed in early September at the request of the president, some groups and video links within the application remain inaccessible.

Tunisia has 12 ISPs. Planet Tunisie, 3S Globalnet, Hexabyte, Topnet, and Tunet are privately owned, while the remaining seven are either wholly or partially owned by the government and tasked with providing internet service to public institutions. The Ministry of Communications Technologies is the main government body for internet technology, and its Tunisian Internet Agency (ATI) is the regulator for all internet-related activities. The law requires all ISPs to obtain a license from the ministry and purchase their bandwidth from the ATI.

Limits on Content

Tunisia's filtering and censorship apparatus is multilayered and extensive. The government employs three main techniques as part of its internet control strategy: technical filtering, postpublication censorship, and proactive manipulation. The government also issues directives to ISPs concerning four types of material that are deemed undesirable and targeted by the authorities: pornography or sexually explicit material, expressions of political opposition to the government, discussions of human rights in Tunisia (including on the websites of many nongovernmental organizations), and tools or technology that enable users to circumvent the government's controls. Directives are not issued to address specific events, since ISPs—along with online news outlets, journalists, and bloggers—are expected to be aware of the standing taboos and deal with new developments accordingly.

[4] http://www.ati.tn/fr/index.php?id=90&rub=27, accessed December 2008
[5] http://www.infocom.tn/index.php?id=268, Accessed on March 23, 2009
[6] "Video-sharing website Dailymotion blocked," *IFEX, April 11, 2007,* http://www.ifex.org/en/content/view/full/82430, accessed on March 23, 2009

All of Tunisia's internet connectivity flows through a single gateway controlled by the ATI. The agency employs SmartFilter software,[7] which allows for key words and phrases to be tagged and filtered throughout the Tunisian internet, including all mail boxes using the .tn country code.[8] Sites that are regularly blocked include opposition sites—such as nawaat.org, reveiltunisien.org, tunisnews.net, and kalimatunisie.com—and the sites of international human rights groups like Freedom House, Reporters Without Borders, Human Rights Watch, and Amnesty International. Many blogs and personal websites are censored and blocked, particularly when they discuss political and social issues. Overseas news outlets such as the British Broadcasting Corporation (BBC) and the *New York Times* are available online, but filtering technology allows the government to block particular pages within these sites. Users are not informed when a site they have attempted to access is blocked. Instead they receive an error message that essentially attributes the failed access attempt to technical problems.[9] According to the OpenNet Initiative (ONI), this falsification stands in contrast to the practices of other states that use SmartFilter software.[10] Virtual Private Networks (VPN) and Secure Sockets Layer (SSL) connections are prohibited without administrative approval. Authorization to acquire SSL certificates and ports to VPNs requires extra payment and is only given to offshore companies.

Postpublication censorship can take a number of forms. Individual blog entries may be deleted, in most instances within 24 to 48 hours of their posting. In other cases, entire blogs may be shut down by service providers. Search engines, including the forthcoming google.com.tn, filter results to exclude those that are censored or that do not favor the Tunisian government's perspective.

In addition to preventing certain content from appearing in Tunisian cyberspace, the government has recently begun to proactively shape public opinion online. In 2007 it put together a small group of people to visit websites and actively guide discussion in a progovernment direction. The authorities have also extended their control over traditional media to the online environment by strongly encouraging, but not forcing, news portals to obtain their articles from Tunisia Africa Press, the official state news agency, enabling the official version of events to dominate.

Although the Tunisian blogosphere is still young (effectively started in 2006) and comparatively small (600 active blogs), it serves as a dynamic alternative forum for the practice of free speech. Blogs have begun to play an important role in addressing issues and events that are considered to lie beyond the "red lines" observed by traditional media, such as the labor riots that took place in the Gafsa mining area in early 2008.[11] Videos and press reports were published online on a daily basis, and a blog was created to gather all the information related to this event. Blogs covering red-line issues always find themselves censored eventually, but the deterrent effect is negligible, as bloggers simply move their blogs to another site. Some bloggers have started as many as nine blogs in an attempt to maintain their outlet in the face of persistent censorship. Others have developed more creative techniques. The blog *NormalLand* discusses Tunisian politics by using a virtual country with a virtual leader, and with various government positions being assigned to other

[7] SmartFilter technology is provided to the Tunisian government by US company Secure Computing.

[8] "Internet Filtering in Tunisia in 2005: A Country Study", *Open Net Initiative*, http://cyber.law.harvard.edu/oni-tunisia/ , accessed on March 26, 2009

[9] http://www.nawaat.org/portail/2006/06/13/tunisie-le-scandale-de-la-403-maquillee-en-404/ , accessed on March 26, 2009

[10] "Internet Filtering in Tunisia in 2005: A Country Study", http://cyber.law.harvard.edu/oni-tunisia/ , accessed on March 26, 2009

[11] "Silencing online speech in Tunisia", *Global Voices*, August 20, 2008, http://globalvoicesonline.org/2008/08/20/silencing-online-speech-in-tunisia/ , accessed on March 26, 2009

Tunisian bloggers. *NormalLand* even has its own flag and national anthem modeled after the actual Tunisian versions.[12]

In December 2008, bloggers pushed back against encroaching censorship with a vocal protest against the Tunisian Blog Awards. The awards were intended to honor the vibrancy and diversity of the Tunisian blogosphere, but the organizers of the event enlisted sponsors who insisted on excluding any blog that was deemed to have a "hateful, racist or religious character or those that spread ideas against common morals, the public order, prevailing laws and regulations." This automatically removed from competition many popular blogs, including any that were judged to have been critical of Tunisia's politics or human rights record.[13] Despite the bloggers' protest, minority groups and local nongovernmental organizations have not yet started to use the internet as a mobilization tool.

Violations of Users' Rights

Tunisian law allows the government to block or censor internet content that is deemed obscene or threatening to public order, or is defined as "incitement to hate, violence, terrorism, and all forms of discrimination and bigoted behavior that violate the integrity and dignity of the human person, or are prejudicial to children and adolescents."[14] In December 2003, the authorities adopted an antiterrorism law that is vaguely worded and can be applied to internet use. It created summary procedures for bringing terrorism suspects to trial, and stipulated that these procedures would also apply to those accused of "inciting hate or racial or religious fanaticism whatever the means used."

The government also frequently uses ordinary criminal charges, such as sexual harassment and defamation, to oppress online journalists and bloggers. The most widely known example is the case of the lawyer and human rights defender Mohammed Abbou, who was arrested on defamation charges and sentenced in March 2005 for an online article in which he compared the torture of political prisoners in Tunisia to the abuses committed by American soldiers in Abu Ghraib, Iraq. He was released in July 2007, but he continued to face threats and intimidation, and the authorities have refused to allow him to leave the country. Blogger and online journalist Omar Mestiri was brought to trial on defamation charges in August 2007 for an article he wrote for a French website; the piece was never even available in Tunisia, since the government actively blocks the website.[15] In November 2007, blogger and journalist Slim Boukhdhir was arrested and charged with aggression against a public employee and violation of public morality standards. He was sentenced to one year in prison,[16] but he was unexpectedly released in July 2008 after serving only seven months.[17] In 2008,

[12] "Tunisphere: How to blog about politics without being censored", *Global Voices*, February 27, 2007,http://globalvoicesonline.org/2007/02/27/tunisphere-how-to-blog-about-politics-without-being-censored/ , accessed March 26, 2009

[13] "Furor over Tunisian Blog Awards Censorship", *Global Voices*, December 14, 2008, http://globalvoicesonline.org/2008/12/14/furor-over-tunisian-blog-awards-censorship/, accessed on March 26, 2009

[14] "2008 Human Rights Practices: Tunisia", *U.S. Department of State*, February 25, 2009, http://www.state.gov/g/drl/rls/hrrpt/2008/nea/119128.htm, accessed on March 26, 2009

[15] "IFEX-TMG Calls For Libel Charges to be Dropped Against Journalist", *IFEX*, August 21, 2007,http://www.ifex.org/en/content/view/full/85730 , accessed on March 26, 2009 (The case was dismissed after the plaintiff retracted the charges.)

[16] "Journalist given one year sentence in 'unfair trial'", *IFEX*, December 11, 2007, http://www.ifex.org/en/content/view/full/88580 , accessed on March 26, 2009

[17] "Journalist Slim Boukhdhir released from Tunisian prison", *Magharebia*, July 23, 2008, http://www.magharebia.com/cocoon/awi/xhtml1/en_GB/features/awi/features/2008/07/23/feature-01 , accessed on March 26, 2009

blogger Ziad el-Heni filed the first-ever lawsuit against the ATI, claiming that the agency practiced illegal censorship and violated his right to free expression by blocking Facebook in August 2008.[18] The case was dismissed by the Third District Court in November 2008, and there is currently no avenue open to appeal this decision.

Anonymity and the right to privacy are nonexistent concepts in Tunisia. While the government does not expressly forbid anonymity and users can post anonymous comments on websites, the government has access to user information through ISPs and can track the comment to the poster. By law each ISP must submit a list of its subscribers to the ATI on a monthly basis.[19] Publinets are also monitored. Under Tunisian law, the managers are responsible for customers' web-browsing habits and activities. It is common to see the owners asking customers not to visit some sites. Posters displayed on the premises remind users that pornographic and other objectionable sites are prohibited. It is necessary to present an identity card to use Publinet facilities, and the managers have the right to access anything saved to disk by their customers.[20] Users are also required to present personal information prior to purchasing a mobile phone or SIM card, and SMS (text messaging) is monitored for red-line or taboo topics in much the same way as the internet.

Extralegal intimidation and physical violence targeting online journalists and bloggers is common practice in Tunisia. Sihem Bensedrine, editor in chief of the online news site Kalima, has been menaced for years by physical intimidation and smear campaigns; the site itself has been blocked since 1999. Between October 2008 and the end of the year, there were six reported instances of harassment against her employees at Kalima.[21] Ziad el-Heni, the journalist and blogger, has been censored eight times and faces frequent intimidation and occasional physical aggression. Slim Boukhdhir, in addition to having been arrested for his writings, has been repeatedly harassed by state officials; this reportedly included abuse and threats by prison guards during his seven months behind bars.[22] Recently, targeted technical attacks have become a popular tool for intimidating and silencing ICT users.[23] In July 2007, Slim Boukhdhir's blog was hacked and deleted. In October 2008, an attack on kalimatunisie.com destroyed all content on the site, forcing it to be entirely rebuilt. E-mail hacking is also common; accounts that have no secured access are monitored, and important information may suddenly disappear. These processes are meant to gradually discourage bloggers and online journalists who dare to criticize the government's policies. Tunisians who wish to explore the internet and visit censored websites are forced to use proxies and anonymizers. However, proxies are continuously "blacklisted" by the Tunisian government, and users risk potential harm if they are caught searching for or using this technology.

---

[18] "Journalist sues Tunisian Internet agency for censorship", *Magharebia*, September 15, 2008, http://www.magharebia.com/cocoon/awi/xhtml1/en_GB/features/awi/features/2008/09/15/feature-01 , accessed on March 26, 2009

[19] "2008 Human Rights Practices: Tunisia", http://www.state.gov/g/drl/rls/hrrpt/2008/nea/119128.htm , accessed on March 26, 2009

[20] "Internet Filtering in Tunisia in 2005: A Country Study", http://cyber.law.harvard.edu/oni-tunisia/ , accessed on March 26, 2009

[21] "Smear campaign against Ms. Sihem Bensedrine", *International Federation for Human Rights*, January 6, 2009, http://www.fidh.org/Smear-campaign-against-Ms-Sihem , accessed on March 26, 2009

[22] "Tunisia: Relentless campaign against imprisoned blogger and journalists Slim Boukhdhir", *Global Voices*, March 24, 2008,http://globalvoicesonline.org/2008/03/24/tunisia-relentless-campaign-against-imprisoned-blogger-and-journalist-slim-boukhdhir , accessed on March 26, 2009

[23] "Kalima website targeted; police attack OLPEC secretary general",*IFEX*, October 14, 2008, http://www.ifex.org/en/content/view/full/97591 , accessed on March 26, 2009

Turkey

Status: Partly Free

Obstacles to Access: **11** (0–25)
Limits on Content: **13** (0–35)
Violations of User Rights: **16** (0–40)
Total Score: **40** (0–100)

Population: 75.8 million
Internet Users/Penetration 2006: 10.2 million / 14 percent
Internet Users/Penetration 2008: 26.5 million / 37 percent
Mobile Phone Users/Penetration 2006: 52.7 million
Mobile Phone Users/Penetration 2008: 62.8 million
Freedom of the Press (2008) Score/Status: 51 / Partly Free
Digital Opportunity Index (2006) Ranking: 52 out of 181
GNI Per Capita (PPP): $12,300
Web 2.0 Applications Blocked: Yes
Political Content Systematically Filtered: No
Bloggers/Online Journalists Arrested: No

Introduction

Internet and mobile-telephone use in Turkey has grown significantly in recent years, though access remains a challenge in some parts of the country, particularly the southeast. The government adopted a hands-off approach to regulation of the internet until 2001, but it has since taken steps to limit access to certain information and blocked hundreds of websites, including some carrying political content. A related and significant threat to online freedom has been the repeated blocking of advanced web applications, particularly video-sharing sites like YouTube. Nevertheless, 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.

Internet use in Turkey became popular in the mid-1990s with the introduction of home dial-up connection services. Since then, the number of dial up users—and since 2006 the number of ADSL users—has grown considerably. The government in February 2003 launched the E-Transformation Turkey Project, which aims to ensure the transition to an information society.

Obstacles to Access

Despite an increasing penetration rate in the last few years, obstacles to internet access remain. According to the International Telecommunication Union (ITU), Turkey had approximately 26.5 million internet users as of March 2008, for a 36.9 percent penetration rate.[1] In 2008, the total number of mobile-phone subscribers reached 63.6 million, for a penetration rate of 90 percent. There were an estimated 3.2 million broadband connections as of September 2007. Although many people access the internet from workplaces, universities, and internet cafes, poor infrastructure—including limited telecommunication services and even lack of electricity in certain areas, especially in the eastern and southeastern regions—has a detrimental effect on citizens' ability to connect, particularly from home. High prices, most notably for broadband, and a lack of technical literacy, especially among older Turks, are also significant factors. According to a 2006 State Planning

[1] Internet World Stats, http://www.internetworldstats.com/europa2.htm#tr, accessed January 2009 – based on International Telecommunications Union (ITU) data

Organization Report,[2] the problem of developing technical competency is greater than the challenges related to cost, which has been decreasing in recent years.[3]

The population generally enjoys widespread access to internet technology, but the government routinely blocks advanced web applications. Incidents of access restrictions on video-sharing sites such as YouTube, Kliptube, and Dailymotion, as well applications such as Wordpress, Blogspot, Google groups, and the photo-sharing website Slide have become regular occurrences, particularly in 2008. In the case of YouTube alone, access was blocked 11 times during the year, and the last block was still in force at year's end. In most instances, these large-scale shut downs have been blunt efforts to halt the circulation of specific content that is deemed undesirable by the government.

There are 97 internet-service providers (ISPs) in Turkey, but the majority act as resellers for the largest, Turk Telekom, which provides more than 95 percent of the broadband access in the country. The company, which was partially privatized in 2005, still acts as a dominant monopoly in the ISP sector. In addition, liberalization of local telephony is still pending, and the delay undermines competition in the fixed-line and broadband markets. ISPs are required by law to submit an application for an "activity certificate" to a government regulatory body called the Telecommunications Communication Presidency (TIB) before they can offer services. Internet cafes are also subject to regulation and registration. They can only operate after receiving an activity certificate from a local authority representing the central administration. Those that operate without permission may face administrative fines of 3,000 to 15,000 lira ($1,700 to $8,700). Mobile-phone service providers are subject to licensing through a regulatory authority, and a licensing fee set by the Council of Ministers. The Information and Communication Technologies Authority (formerly known as the Telecommunications Authority) and the TIB, which it oversees, act as the regulators for all of these technologies and are well staffed and self-financed.[4] However, the fact that board members are government appointees is a potential threat to the authority's independence, and its decision-making process is not transparent. Nonetheless, there have been no reported instances of activity certificates being denied.

Limits on Content

Government censorship of the internet continues to be relatively common and has increased in the recent past, sometimes targeting political content. The procedures surrounding decisions to block websites, whether by the courts or the TIB, remain nontransparent, creating significant challenges for those seeking to appeal. In May 2007, the government enacted Law No. 5651, entitled "Regulation of Publications on the Internet and Suppression of Crimes Committed by Means of Such Publication."[5] This law established the responsibilities of content providers, hosting companies, mass-use providers, and ISPs. Its most important provision allows the blocking of websites containing certain types of content, including material that shows or promotes sexual exploitation and abuse of children, obscenity, prostitution, and gambling. Also targeted for blocking are websites deemed to involve crimes committed against Mustafa Kemal Ataturk, modern Turkey's founding father. Domestically hosted websites with proscribed content can be taken down, and those based abroad can be blocked and filtered through ISPs. The result has been the blocking of at

[2] T.R. Prime Ministry, State Planning Organization, Information Society Strategy (2006-2010), July 2006.
[3] *Ibid.*
[4] Information and Communication Technologies Authority, http://www.tk.gov.tr/Eng/english.htm, accessed December 2008
[5] Law No 5651 was published on the Turkish Official Gazette on 23.05.2007, No. 26030.

least 1,310 websites, according to the TIB as of December 1, 2008. Although the available records are limited, the majority of blocks appear to have been on objectively harmful content, but at least 50, and possibly many more, were related to alleged crimes against Ataturk. Some sites are blocked by domain name system (DNS), while others are blocked by both domain name and internet protocol addresses.

The procedure for censoring information under Law No. 5651 lacks transparency and is often done by administrative fiat, or by court orders in other cases. Within the judiciary, blocking orders can be issued by a judge during preliminary investigations as well as during trial. Censorship is also overseen by the TIB, which was established in August 2005 and has been fully functional since July 2006. Under Law No. 5651, the TIB's mandate includes monitoring internet content and executing blocking orders issued by judges and public prosecutors. Moreover, it has been granted its own authority to issue administrative blocking orders for certain content. According to TIB statistics, the courts are responsible for 21 percent of blocked websites, while 79 percent are blocked administratively by the TIB. In some cases, the TIB has successfully asked content and hosting providers to remove offending items from their servers, allowing it to avoid issuing a blocking order that would affect an entire website.

Although Law No. 5651 was designed to protect children from illegal and harmful internet content, its broad application to date has had the effect of restricting adults' access to legal content. In some instances, the courts have blocked websites for political content using laws other than Law No. 5651. For example, Indymedia Istanbul, an independent news outlet that has been active in Turkey since January 2003,[6] had access to its website blocked by a court order in March 2008.[7] The decision was based on Article 301 of the criminal code, which involves insults against "Turkishness."[8] Certain leftist and pro-Kurdish news websites are blocked more consistently, with the latter targeted for containing content that is deemed to favor the Kurdistan Workers' Party (PKK) rebel group or its use of terrorist violence.[9]

The reasoning behind court decisions is not provided in blocking notices, and the relevant rulings are not easily accessible in Turkey. As a result, it is often difficult for site owners to determine why their site has been blocked and which court issued the order, rendering any form of appeal essentially impossible.

Two groups, the All Internet Association (TID) and the Turkish Informatics Association (TBD), have brought cases to the Council of State in an effort to annul all the secondary regulations drawn up on the basis of Law No. 5651 as unconstitutional. The TID has particularly faulted the TIB's authority to issue administrative blocking orders without judicial involvement. The cases were still pending at the end of 2008.

Despite the large number of sites blocked, circumvention techniques and technologies are widely available, enabling even inexperienced users to avoid filters and blocks. Each time a new order is issued and a popular website is blocked, a large number of articles are published to instruct users on how to access the banned websites. This phenomenon is reflected by the fact that YouTube was still the 16th-most-accessed site in Turkey almost three months after the latest blocking order was issued.[10]

---

[6] http://istanbul.indymedia.org/features/english/?l=en, accessed December 2008

[7] Canada NewsWire, "Turkey - Another website blocked in latest of measures that threaten Web 2.0," 01 April, 2008. See further Önderoğlu, E., "Access to Another Website Banned," *Bia News Centre*, 27 March, 2008, at http://www.bianet.org/bianet/kategori/english/105906/access-to-another-website-banned, accessed December 2008

[8] Article 301 (Insulting Turkishness, the Republic, the organs and institutions of the State).

[9] Reporters sans frontiers, "Illegal court ban on websites deplored" 08 April 2008, http://www.rsf.org/article.php3?id_article=26484, accessed December 2008

[10] According to the alexa.com website on 18 August, 2008

Turkish users are increasingly relying on internet-based publications as a primary source of news. Advanced applications like Facebook, YouTube (despite being banned since May 2008), Twitter, MySpace, and blogging services such as Blogger, Blogspot, and Wordpress are extremely popular in Turkey. In August 2008, in a show of solidarity and protest over the government's repeated blocking of various websites and applications, nearly 200 Turkish blogs temporarily shut themselves down and posted a message that read "This site is blocked by [the author's] own choice." Instructions were provided to bloggers on how to convert their sites to "blocked" pages, and bloggers who participated said the campaign was designed "to show Turkish Web surfers what the Internet would look like if censorship continues unabated."[11] There is a wide range of blogs and websites on which citizens question and critique Turkish politics and leaders, including on issues that are generally deemed to be politically sensitive. For example, a website called Ozurdiliyoruz.com was recently set up to offer an apology for "the insensitivity showed to and the denial of the Great Catastrophe that the Ottoman Armenians were subjected to in 1915." There are currently more than 28,000 signatories on the apology letter. The majority of civil society groups in Turkey maintain an online presence, and social-networking sites are used for a variety of functions, including political campaigns. Thus far, however, mobile phones and SMS (text messaging) technology do not seem to play a large role in social or political mobilization.

Violations of Users' Rights

The constitution includes broad protections for freedom of expression, stating that "everyone has the right to express and disseminate his thought and opinion by speech, in writing or in pictures or through other media, individually or collectively." Turkish law and court judgments are also subject to the European Convention on Human Rights and bound by the decisions of the European Court on Human Rights. While many hundreds of websites have been blocked under Law No. 5651, there have been no prosecutions of individuals for publication of the proscribed content. There are no laws specifically criminalizing online expression or activities like posting or downloading information, sending e-mail, or transmitting text messages. However, many provisions of the criminal code and other laws, such as the Anti-Terrorism Law, are applicable to both online and offline activity. These include the ban on encouragement or assistance of crimes against Ataturk. Furthermore, Article 301 allows prison terms of six months to three years for "the denigration of Turkishness." It has been used against journalists who assert that genocide was committed against the Armenians in 1915, discuss the division of Cyprus, or write critically about the security forces. Book publishers, translators, and intellectuals have also faced prosecution for insulting Turkish identity.[12] Thus far there have been no prosecutions under Article 301 for online material, but the possibility of such charges significantly contributes to self-censorship.

The constitution states that "secrecy of communication is fundamental," and users are allowed to post anonymously online. The constitution also specifies that only the judiciary can authorize interference with the freedom of communication and the right to privacy. For example, judicial permission is required for technical surveillance under the Penal Procedural Law. However, the anonymous purchase of mobile phones is not allowed, and would-be buyers need to provide official identification. The use of encryption is currently not prohibited or regulated by law, and Turkey has no data protection law.

[11] Global Voices Online, "Bloggers Banning Themselves," August 18, 2008 http://globalvoicesonline.org/2008/08/18/turkey-is-typingbloggers-banning-themselves/, accessed March 20, 2009

[12] Freedom of the Press, Turkey (2008), http://www.freedomhouse.org/template.cfm?page=251&year=2008, accessed March 30, 2009

Despite the constitutional protections, the right to privacy and private communications remains rather problematic. In practice, most forms of telecommunication have been tapped and intercepted.[13] During 2008, several surveillance scandals received widespread media attention, and it has been alleged that all communications are subject to interception by various law enforcement and security agencies, including the Gendarmerie (military police). Some have reported that up to 50,000 phones—both mobile and land-line—are legally tapped daily in Turkey, and 150,000 to 200,000 interception requests are made each year.

Such actions have been challenged in court on at least one occasion. In June 2008, the Ankara 11th High Criminal Court initially granted both the Gendarmerie and the National Intelligence Agency (MIT) the authority to view countrywide data traffic retained by telecommunication-service providers. The TIB lodged two complaints with the court and asked the Ministry of Justice to clarify the permission granted to the Gendarmerie. Subsequently, the Supreme Court of Appeals overruled the Ankara court's decision and stated that "no institution can be granted such authority across the entire country, viewing all people living in the Republic of Turkey as suspects, regardless of what the purpose of such access might be."[14] Nonetheless, similar powers to access and monitor data traffic have been granted to the MIT as well as the National Police Department. Faced with criticism over these powers, the parliament in 2008 launched a major inquiry into illegal surveillance and interception of communications, and the inquiry will continue into 2009.

ISPs are required to take down, to the extent that it is technically possible, any illegal content published by their customers once it has been identified by the TIB or in a court order. Providers are not required to monitor the information that goes through their networks, nor do they have a general obligation to seek out illegal activity. In terms of data retention, access providers are required to retain all communications (traffic) data for a period of one year from the date of the communication, while maintaining its accuracy, security, and integrity. Administrative fines of 10,000 to 50,000 lira ($5,800 to $30,000) can be imposed on access providers if they fail to comply, but to date no ISP or other provider has been prosecuted.

Internet cafe operators are required under Law No. 5651 to deploy and use filtering tools to block access to content that is deemed illegal. Under related regulations, they are also required to record daily the accuracy, security, and integrity of retained data using software provided by the TIB, and to keep this information for one year.[15] All mass-use providers are required to use one of the filtering programs approved by the TIB, which are published on the TIB's website. However, criteria for the approval are not known or publicly available. Nor is it clear whether the approved programs filter websites other than the ones blocked by the courts and the TIB. Since the procedure is not transparent and remains open to abuse, the TIB's filter approval system could lead to systematic censorship of certain websites without the necessary judicial or TIB orders.

There were no reports of extralegal intimidation or harassment of bloggers or others for their online activities, though some internet content was believed to have contributed to the murder of print journalist Hrant Dink in January 2007. Dink was a prominent member of the Armenian minority in Turkey, and editor in chief of the bilingual Turkish-Armenian newspaper *Agos*. Prior to his assassination, he had received several death threats via e-mail. It was reported that his killer was influenced by the writings on certain racist websites and online forums. Such sites are not covered

[13] For a history of interception of communications see Bildirici, Faruk, *Gizli Kulaklar Ulkesi* (The Country of Hidden Ears), Istanbul: Iletisim, 1999. See further Coskun, Enis, *Kuresel Gozalti: Elektronik Gizli Dinleme ve Goruntuleme*, Ankara: Umit Yayincilik, 2000

[14] Zaman, "Supreme Court of Appeals overrules gendarmerie call detail access," 06 June, 2008

[15] See Law No. 5651, article 10 (4)(ç) and (e)

by Law No. 5651 and have not been subject to blocking or regulation. While Dink's murder may have been fueled by anti-Armenian sentiment among Turks online, the first major reaction to his death came from Turkish bloggers, who expressed their sadness and regret at the loss of a fellow Turkish journalist in a senseless act of violence.[16]

Physical violence is not a major threat to Turkish users, but technical attacks are becoming increasingly common. In July 2008, the websites of a free speech organization (www.antenna-tr.org and www.orrtakpayda.org) run by activist and musician Sanar Yurdatapan were attacked by a group of Turkish nationalist hackers. An investigation was launched, but it did not lead to arrests or prosecutions. Continual attacks by hackers are thought to be partly responsible for the apparent decline of the Kurdish blogosphere. According to GlobalVoices, the site IraqiKurdistan has been hacked by a character who names himself the 'dangerous ghost ne mutlu turkum diyene' and it is believed that the site From Holland to Kurdistan switched its blog to invited readers only because of similar attacks.[17] Domain hijacking also remains popular with Turkish hackers, who allegedly targeted the European Commission[18] and PKK websites, among others, during 2008.[19] They are known to engage in minor cyberwars with their Greek counterparts as well.

[16] Global Voices Online, "Caucasus Blog Review," December 31, 2007, http://globalvoicesonline.org/2007/12/31/caucasus-2007-blog-review/, accessed March 20, 2009, and "Notes From the Turkish Blogosphere," January 20, 2007, http://oneworld.blogsome.com/2007/01/20/notes-from-the-turkish-blogosphere-on-hrant-dinks-murder/, accessed March 20, 2009

[17] Global Voices Online, "The State of Kurdish Activism," July 10, 2007, http://globalvoicesonline.org/2007/07/10/kurdistance-the-state-of-kurdish-activism/, accessed March 20, 2009

[18] See Turkish Hacker Group Strikes Again, This Time Victims are ICANN and IANA, 27 June, 2008, at http://www.circleid.com/posts/86272_turkish_hackers_strike_again_icann_iana/, accessed December 2008

[19] See Turkish hacker group "AyYildiz Team" threatens Europe, 14 July, 2008, at http://en.apa.az/news.php?id=52032, accessed December 2008

United Kingdom

Status: Free

Obstacles to Access: **0** (0–25)
Limits on Content: **6** (0–35)
Violations of User Rights: **14** (0–40)
Total Score: **20** (0–100)

Population: 61 million
Internet Users/Penetration 2006: 37.5 million / 62 percent
Internet Users/Penetration 2008: 43.9 million / 72 percent
Mobile Phone Users/Penetration 2006: 69.8 million
Mobile Phone Users/Penetration 2008: 72 million
Freedom of the Press (2008) Score/Status: 18 / Free
Digital Opportunity Index (2006) Ranking: 10 out of 181
GNI Per Capita (PPP): $33,800
Web 2.0 Applications: No
Political Content Systematically Filtered: No
Bloggers/Online Journalists Arrested: No

Introduction

Access to the internet and digital media technologies in the United Kingdom is among the best in the world. Nonetheless, potential threats to users' rights to information and privacy have emerged in recent years, particularly as a result of inadequate transparency in the blocking of harmful content and extensive data retention. The first mobile-telephone call was made on January 1, 1985, and internet use became popular in the mid-1990s, though academic institutions had access prior to that.

The British experience has also raised concerns over the role of private actors, such as internet-service provider (ISP) associations, in the regulation and blocking of internet content, particularly when these self-regulatory mechanisms lack sufficient transparency and public oversight and when companies are susceptible to influence by powerful economic interests. An erosion of government observance of civil liberties since September 11, 2001 has also affected internet freedom and the right to privacy in general.

Obstacles to Access

The United Kingdom enjoys widespread internet access, including broadband, which is available even in rural areas and has been expanding in recent years. As of June 2008, the country had an estimated internet-penetration rate of 68.6 percent. In 2007, more than 86 percent of computer owners had a broadband connection, compared with 73 percent in 2006. Research suggests that high-speed internet is available to almost everyone, although the connection speed may vary according to the user's distance from the exchange and the quality of the local network.[396]

The percentage of consumers who did not have an internet connection for involuntary reasons such as cost decreased to just 8 percent in 2007. This decline may stem from the introduction of bundled services, competing offers, and lower prices, coupled with "free" services awarded by some operators (Orange, Sky, TalkTalk, and others) when customers accept additional services such as line rental and mobile contracts.

Mobile-phone penetration is also extensive, with the number of mobile connections exceeding the total population. In 2006, the country had the second-highest penetration of mobile

[396]See generally Ofcom, The Consumer Experience Research Report 08, at http://www.ofcom.org.uk/research/tce/ce08/, accessed March 30, 2009

connections per head in Europe. Many individuals own more than one mobile phone, and the average is 1.44 subscriptions each.[397] In 2007, household subscriptions to mobile-phone service exceeded fixed lines for the first time. While 16 percent of the population still does not own mobile phones, most in this group are either very young, very old, or too poor to do so.[398] Mobile phones with both second generation (2G) services, including SMS (text messaging), and third generation (3G) features, including high-speed internet and multimedia capabilities, are available to the majority of the population.

The government does not place limits on the amount of bandwidth ISPs can supply, and the use of internet infrastructure is not subject to governmental control. Internet protocols and tools such as Voice over Internet Protocol (VoIP), peer-to-peer (P2P) networks, and advanced web applications are not subject to blocking. For example, the YouTube video-sharing site, the social-networking site Facebook, and international blog-hosting services are freely available. Users also have access to circumvention technologies, which they employ most often in workplaces or universities that have installed filtering tools and software.

The United Kingdom provides a competitive market for internet access, with approximately 700 ISPs in operation. ISPs are not subject to licensing but must comply with the general conditions set by the Office of Communications (Ofcom), such as having a recognized code of practice and being a member of an alternative dispute-resolution scheme. Prior to July 2003, any mobile-phone company operating in the country had to obtain a license under the Telecommunications Act of 1984. In 2003, however, this arrangement was replaced by the General Authorization regime, under which licenses are no longer required for providing communications networks or services, and everyone is "generally authorized" to do so.[399] Major mobile-phone providers, such as Vodafone, Orange, T-Mobile, and O2, operate on this basis.

Ofcom is the independent regulator and competition authority for general communications industries, including telecommunications and wireless communications services. Ofcom is generally viewed as fair and independent in its oversight. Its main legal duties are to ensure that the United Kingdom has a wide range of electronic communications services, including high-speed or broadband information services.

Limits on Content

While access to online content, including that addressing domestic politics and human rights violations, is extensive and free of significant barriers, some restrictions exist on terrorism-related content, and in at least one incident during the coverage period, private actors' interests led to the removal of information that was potentially beneficial to the public. In addition, it is estimated that thousands of websites containing content harmful to children have been blocked. The lack of transparency surrounding such censorship practices has raised concerns over the room for abuse, particularly as these actions are usually carried out by private-sector actors with little public oversight.

British law does not provide for blocking or filtering websites, blogs, or any other type of internet communication for the purposes of limiting political and social content. Censorship systems instead focus on extreme pornography, racial hatred, and material that is harmful to children. Politics, foreign news, human rights, and religious content are not blocked. The country's content

[397] Deloitte "Total Mobile – The Digital Index" January 2009
[398] Deloitte "Total Mobile - The Digital Index" January 2009
[399] The General Authorisation Regime, http://www.ofcom.org.uk/telecoms/ioi/g_a_regime/, accessed March 30, 2009

regulation policy is generally in line with that of the European Union. Although the United Kingdom also signed the Cybercrime Convention developed by the Council of Europe, it has yet to ratify it.

As Ofcom is not empowered to deal with internet content regulation, self- and co-regulatory initiatives are in place to tackle illegal and harmful material. Britain's Internet Services Providers' Association (ISPA) adopted a code of practice in January 1999, which refers to the work of the Internet Watch Foundation (IWF).[400] The IWF is responsible for informing all British ISPs of allegedly illegal content, which they are then required to remove from websites, newsgroups, and servers.[401] The IWF launched a hotline for reporting illegal material on the internet in December 1996, and the foundation received charitable status in 2005. It is fully funded and supported by British ISPs, which oversee its operation. Members of the ISPA are required to adhere to all IWF procedures. The IWF reportedly orders blocking of some 10,000 web pages from around the world every year,[402] and the list can contain between 800 and 1,200 live URLs at any given time.[403] Most of the content blocked or taken down includes pornography, particularly involving children, or information inciting racial hatred. Content that involves state secrets or is subject to contempt of court laws is also taken down by ISPs or removed from search engines.

British Telecom (BT) has partnered with the IWF to create the CleanFeed filtering system, which blocks access to any images or websites listed in the IWF database. While British ISPs are under no legal obligation to implement such a system or to monitor their own systems, it is estimated that the country's largest ISPs were either currently filtering or had plans to begin filtering by the end of 2006.[404] Providers can face prosecution if they are found to have had knowledge of illicit material, including defamatory content and terrorist propaganda, but failed to remove it.[405]

While the IWF's blocking and removal actions focus mainly on legitimately harmful content, its procedures and policies are not transparent. The blocking criteria lack clarity, and the internal appeal process is inadequate. There is no judicial or governmental oversight of the IWF's activities, and critics have argued that this leaves the body with too much discretion. In a case that received widespread attention, the IWF in December 2008 added the Wikipedia page devoted to the rock band Scorpions to its blocking list. The page featured an image from the band's controversial 1976 album, Virgin Killer, which consisted of "a striking photograph of a nude, pre-pubescent girl covered by broken glass."[406] After the image was reported to the IWF, the page—including the text—was blocked through BT's CleanFeed technology.[407] In some cases, British users were temporarily unable to see or edit any Wikipedia content.[408] While the IWF subsequently revoked its decision after protests from the Wikimedia Foundation, the act of censorship led the British public to question the IWF's ability as a private body to both control internet content and obstruct public access.

[400] ISPA Code of Practice, www.ispa.org.uk/about_us/page_16.html, accessed March 30, 2009
[401] See section 5 of the ISPA Code of Practice
[402] Ibid.
[403] IWF Facilitation of the Blocking Initiative, http://www.iwf.org.uk/public/page.148.htm, accessed March 30, 2009
[404] Child Abuse (Internet), House of Commons Hansard Written Answers for 15 May, 2006
[405] Section 1, Defamation Act 1996
[406] The Observer, "Wikipedia censorship highlights a lingering sting in the tail," 14 December, 2008
[407] The Guardian, "Wikipedia row escalates as internet watchdog considers censoring Amazon US over Scorpions image,"8 December, 2008
[408] Ibid.

The Terrorism Act of 2006 contains provisions that criminalize the encouragement of terrorism,[409] as well as the dissemination of terrorist publications.[410] There are procedures for notification and removal if such activities are carried out over the internet.[411] While the content in question may be legitimately harmful, the current policies and legislation have decreased judicial oversight. Any British police officer is empowered to issue the removal notices, though their preferred method is to first use informal requests to service providers. According to the secretary of state for the Home Office, Jacqui Smith, "to date this has proved effective," but statistics on the number of sites removed through such informal contact are not available.

In a different form of censorship via private actors, economic pressure from powerful individuals has led to the removal of content that the public may have an interest in accessing. In October 2007, an ISP shut down a blog it hosted after lawyers representing Russian-based business magnate Alisher Usmanov, a key shareholder of Arsenal Football Club in the United Kingdom, threatened to sue the provider for defamation if it did not remove certain content from the blog. The site belonged to the former British ambassador to Uzbekistan, Craig Murray, and raised questions about Usmanov's past, his ties to Uzbekistan's authoritarian president, and accusations that he had engaged in criminal behavior. When the ISP, Fasthost, deactivated Murray's blog, however, it also shut down servers hosting a dozen other sites, including the blog of former member of Parliament and now mayor of London Boris Johnson. Murray eventually restarted his blog through another ISP based in the Netherlands.[412]

Because the IWF has mainly concentrated on the availability of child pornography, users in the United Kingdom continue to enjoy wide access to free or low-cost blogging services, allowing them to express their views on the internet. Users and nongovernmental organizations also employ various forms of online communication to organize political activities, protests, and campaigns. Almost all political and religious views are represented through blogs and popular social-networking sites such as Facebook. Civil society organizations maintain a significant presence online and have used internet platforms to promote various causes, such as the NO2ID (http://www.no2id.net/) campaign to raise awareness on the use of identity cards and the creation of a "database state" in Britain.

---

[409] *Terrorism Act 2006* (U.K.), 2006, c. 11, s. 1: "This section applies to a statement that is likely to be understood by some or all of the members of the public to whom it is published as a direct or indirect encouragement or other inducement to them to the commission, preparation or instigation of acts of terrorism…." In July 2007, three men were found guilty and sentenced to a total of 24 years in prison for incitement to commit an offense of terrorism, namely murder, through the internet. Younes Tsouli, Waseem Mughal, and Tariq al-Daour were convicted at Woolwich Crown Court after using websites to incite other Muslims to wage war on nonbelievers. The judge stated that "while some of this material might in future cases properly found a prosecution under those sections of the Terrorism Act 2006 which prohibits conduct which indirectly encourages or glorifies terrorism, much of it went a good deal further than that and amounted to an incitement to commit murder." See *Attorney General's References (Nos 85, 86 and 87 of 2007) R v Tsouli and others*, [2007] EWCA Crim 3300.

[410] *Ibid.*, s. 2(2): dissemination of terrorist publications includes: distributing or circulating a terrorist publication; giving, selling, or lending such a publication; offering such a publication for sale or loan; providing a service to others that enables them to obtain, read, listen to or look at such a publication, or to acquire it by means of a gift, sale or loan; transmitting the contents of such a publication electronically.

[411] *Ibid.* ss. 3, 4

[412] http://www.timesonline.co.uk/tol/news/politics/article2508108.ece, and http://www.iht.com/articles/2007/10/07/business/net08.php/, accessed December 2008

Violations of Users' Rights

Established law provides for freedom of expression in the United Kingdom, and the government generally respects this right in practice. There were no reports of bloggers being arrested during the coverage period, but other infringements on user rights, such as libel tourism and extensive surveillance, remain a concern.

While there is no explicit constitutional protection for freedom of speech, the Human Rights Act of 1998 provided for limited incorporation of the European Convention on Human Rights (ECHR) into the legal system. Therefore, such rights as freedom of expression and privacy are protected under British law. Nevertheless, freedom of expression has been threatened by the growth of libel tourism, whereby litigants from foreign countries use favorable libel laws in the United Kingdom to silence and intimidate journalists and other content producers. This practice has resulted in self-censorship, particularly on issues related to the funding of terrorism. As the law stands, anyone in the world can sue for libel in a British court as long as the material has been accessed in Britain. British judges have accepted lawsuits on this basis even when the number of hits for the online content in question is extremely small and it is available only in a foreign language, or if only several copies of a book have been bought from an online vendor by customers based in the UK. Those accused of libel in such cases are often small, non-British organizations or authors who cannot bear the cost of litigation and find themselves facing powerful foes with no such limitations.[413]

In 2007, the Ukrainian tycoon Rinat Akhmetov sued several Ukrainian news outlets, including the online Ukranian-language Obozrevatel, under British libel laws, claiming that the organizations had published false allegations against him. A judgment was issued in default, and Obozrevatel was ordered to pay Akhmetov $75,000.[414] The Saudi billionaire Sheik Khalid bin Mahfouz has filed more than 30 libel suits in London against authors and publishers in the United States and Europe. Such cases have had a dramatic effect on investigative journalists, researchers, and publishers, who fear expensive litigation and harsh penalties for publishing critical material. Cambridge University Press removed the book *Alms for Jihad: Charities and Terrorism in the Islamic World* by J. Millard Burr and Robert O. Collins from circulation after the threat of a libel suit by bin Mahfouz.[415] Libel tourism not only threatens to suppress public debate on international security issues like terrorism, it may also restrict human rights groups in their reporting, especially when dealing with violent and repressive regimes.

While anonymity in online communication is generally guaranteed, there are some limitations on anonymous expression, especially for mobile-phone users. Customers are not permitted to purchase mobile phones anonymously, and names and addresses are required for prepaid phone services. Internet users can post comments anonymously on various forums, but courts have the power to compel forum operators or ISPs to provide the personal details of those users,[416] and ISPs have been ordered to do so in a number of libel cases.[417]

Encryption technology is allowed in the country, but law enforcement agencies can demand the decryption of data or production of decryption keys under new provisions of the 2000 Regulation of Investigatory Powers Act (RIPA) that took effect on October 1, 2007. The Home

[413] *Al Amoudi v. Brisard* [2006] EWHC 1062; [2006] 3 All E.R. 294 (QBD).
[414] "Writ Large," *The Economist*, January 8, 2009, http://www.economist.com/world/international/displaystory.cfm?story_id=12903058, accessed January 2009
[415] Chris Walker, "The globalization of censorship," *International Herald Tribune*, 11 March 2009
[416] Section 35 of the Data Protection Act 35 is used as the legal basis for disclosing the identities of forum users or customers of ISPs.
[417] See *Totalise plc v Motley Fool Ltd and another*, Court of Appeal (Civil Division) [2001] EWCA Civ 1897

Office recently disclosed that eight decryption orders have since been served.[418] Of these cases, the two recipients who refused to comply were prosecuted. In October 2008, the Court of Appeal told two men who had been served notices that they could not rely on their right to silence to refuse to give police their decryption keys.[419]

Concerns about surveillance have grown in recent years, as more data-retention regulations have been imposed on ISPs and the authorities have increasingly used or misused the powers granted under RIPA.[420] The law covers the interception of communications; the acquisition of communications data, including billing data; intrusive surveillance, such as on residential premises or in private vehicles; covert surveillance in the course of specific operations; the use of covert human intelligence sources like agents, informants, and undercover officers; and access to encrypted data.

RIPA enables law enforcement, security, and intelligence agencies to track the associations and interests of internet users through their online communications. The law requires that ISPs maintain reasonable interception capabilities, including systems to record internet traffic on a large scale. ISPs generally retain the addresses of an e-mail's recipient and sender, their digital locations, the subject line of the message, and the time it was sent.[421] The sites that users visit and the times when they log on and off are also recorded. ISPs must be capable of carrying out authorized interceptions within one working day of receiving the order.[422]

In 2007, there were 519,260 requisitions of communications data from telephone companies (including mobile-phone service providers) and ISPs.[423] While the specific content of e-mails can only be obtained with a warrant from the home secretary, RIPA does allow government agencies to access communication records for a variety of reasons, from national security to tax collection. Beginning in January 2009, 792 other organizations—including 474 local councils and every National Health Service trust and fire service—will have the ability under RIPA to access internet traffic information, raising privacy concerns. The actual content of communications, however, would still be inaccessible without approval from the home secretary.

Users who suspect that their communications have been intercepted can submit a formal complaint to the Investigatory Powers Tribunal that explains which ECHR right has allegedly been violated. The tribunal investigates the complaints, and the complainants are entitled to representation at any hearing.[424] In 2007, the tribunal received 66 complaints. The Office of Surveillance Commissioners oversees the officials who authorize and conduct covert surveillance operations and use human intelligence sources.[425] It is tasked with inspecting and reporting operations that fail to comply with RIPA. The commissioners are appointed by the prime minister,

[418] See RIPA Part III Section 49 Notices, 02 May, 2008, http://cyberlaw.org.uk/2008/05/02/ripa-part-iii-section-49-notices/, accessed March 30, 2009

[419] The two men were arrested for helping a third man in a secret house move. The third man was subject to a control order under antiterrorism legislation, which said he could not move house without permission from the authorities. OUT-LAW News, "Court of Appeal orders men to disclose encryption keys." 16 October, 2008, at <http://www.out-law.com//default.aspx?page=9514>.

[420] See generally the Explanatory Notes to Regulation of Investigatory Powers Act at http://www.opsi.gov.uk/acts/acts2000/en/ukpgaen_20000023_en_1, accessed January 2009

[421] Guardian "Prying Eyes"

[422] *Ibid.* para 5.

[423] Guardian "Regulation of Investigatory Powers Act 2000"

[424] Guardian "Security & Privacy"

[425] See, http://www.surveillancecommissioners.gov.uk/, accessed March 30, 2009

but they have nonetheless criticized civil servants for abusing RIPA powers. In 2008, Prime Minister Gordon Brown ordered an inquiry into the rapid increase in the use of RIPA by public authorities.[426]

Despite these complaint and oversight mechanisms, some cause for concern remains. Interception is never revealed to the subject, which may substantially decrease the chances that the Investigatory Powers Tribunal will be alerted to possible abuse or errors in surveillance procedures. Moreover, RIPA stipulates that the contents of an intercepted communication or any related communications data cannot be used as evidence in court, and they are excluded from legal proceedings.

In addition to RIPA, the Antiterrorism, Crime, and Security Act was passed following the terrorist attacks of September 11, 2001. It also requires ISPs to retain communications data and compensates them for the expenses of doing so. Subscriber information and telephony data is retained for a maximum of 12 months.[427] The law allows officers of superintendent or equivalent rank to authorize access to retained data without a judicial or executive warrant, for both national security reasons and minor investigations.[428] The retention time of 12 months may increase to 24 months once the European Union's Data Retention Directive is transposed into British law. While user activities in cybercafés are not subject to monitoring at the point of access, the traffic is recorded as it passes through the ISPs that serve such facilities.

In addition to the current surveillance measures, the government is reportedly planning to introduce a central database for storing the electronic communications traffic data for the country's entire population. The controversial plans, to be published in early 2009, are part of the Intercept Modernisation Programme established by the Home Office and have already been attacked by civil liberty groups for allegedly laying the foundations of a "Big Brother" police state. The Council of Europe's commissioner for human rights, Thomas Hammarberg, has said that British proposals for sweeping powers to collect and store data will increase the risk of the violation of individual privacy rights.[429]

There were no reports during the coverage period of extralegal violence or technical attacks against bloggers or other digital media users, by either state or nonstate actors.

[426] Christopher Hope, "Local Authorities Launched 10,000 Snooping Operations Last Year," July 23, 2008, http://www.telegraph.co.uk/news/uknews/2446314/Local-authorities-launched-10000-snooping-operations-last-year.html, accessed March 30, 2009

[427] A maximum period of six months is required for e-mail data, ISP data, SMS, EMS, and MMS data. On the other hand the draft code requires a maximum retention period of four days for web activity logs. See Home Office, Consultation paper on a code of practice for voluntary retention of communications data, http://www.homeoffice.gov.uk/docs/vol_retention.pdf, 2003, Annex A, Appendix A for further technical details.

[428] Guardian "Prying Eyes"

[429] Verkaik, R., "UK's database plan condemned by Europe." The Independent, 31 December 2008

Glossary

Note: Glossary definitions based on those available from the following sources, as well as additional explanations drawn from other sections of this study: Merriam-Webster Online, www.merriam-webster.com and Webopedia: Online Computer Dictionary for Computer and Internet Terms and Definitions, www.webopedia.com.

Blog: short for weblog, an online personal journal with reflections, comments, and often links to other websites or blogs provided by the writer; most blogs allow reader comments and are used to foster discussion surrounding certain topics; while most contain reflections on bloggers' personal lives, increasingly they are being used to comment on social and political issues

Blogosphere: all of the blogs on the internet or within a specific country, e.g. the Tunisian blogosphere

Broadband: a high-speed internet connection in which a single wire can carry many channels at once, allowing a high data-transfer rate; necessary for viewing multimedia content

Bulletin Board System (BBS): an electronic message center; most bulletin boards serve specific interest groups; users can post information or products for sale, and other posters can respond

Chat Room: an online location that allows multiple users to engage in a real-time, text-based conversation or discussion

Cybercafe: a commercial location where patrons can use the in-house computers to access the internet for a specified fee and time; most often used by travelers or those without a home internet connection

Cyberspace: the nonphysical world created by computer systems; the internet, for example, creates a cyberspace within which people can communicate with one another, do research, or simply window shop; like physical space, cyberspace contains objects (files, mail messages, graphics, etc.) and different modes of transportation and delivery

DDOS Attack: Distributed Denial of Service Attack; generally consists of the concerted efforts of a person or persons to prevent an internet site or service from functioning efficiently or at all, either temporarily or indefinitely; this is usually done by overloading the attacked website with so many requests for information that it crashes and cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable; those responsible often infiltrate computers around the world and program them to join in the assault as an automated network, or "botnet"

Dial-up: an internet connection over a standard telephone line, usually with a very slow speed that makes it difficult to access some features, especially multimedia applications

DNS: domain name system; an internet service that translates domain names—the appellations commonly used to identify websites, e.g., www.example.com—into numerical IP addresses; because domain names are alphabetic, they are easier to remember, but the internet is actually based on IP addresses; every time a user enters a domain name, a DNS service must translate the name into the

corresponding IP address; for example, the domain name www.example.com might translate to 198.105.232.4

DSL and ADSL: digital subscriber line and asymmetrical digital subscriber line; allow data transmission over the wires of a local telephone network, at a faster speed than dial-up permits; the internet connection can be maintained without obstructing telephone use on the same line; ADSL features a greater flow of data in one direction than in the other, so that download speeds are often much faster than upload speeds

Firewall: a system designed to prevent unauthorized access to or from a private network; can be implemented in both hardware and software; all messages entering or leaving the protected network pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria; while in most countries these are also used by companies to prevent employees from accessing content unrelated to their work, in several countries—most notably China and Iran—firewalls are set up on a national level to prevent citizens from accessing certain content from abroad

Forum: an online discussion group in which participants with common interests can exchange open messages; forums are sometimes called newsgroups

Forum Trolling: the practice of lingering in a chat room or forum and reading the posts instead of contributing to the discussion, often used to denote a "spy" who observes what is being said or discussed and then reports that information to authorities or who attempts to maliciously disrupt conversations or agitate users in a forum or chat room

Hosting Service/Host: a service provider that houses, or hosts, multiple websites on its server computers in exchange for a fee

ICT: information and communications technology, including computers and mobile devices

Instant Messaging/I-Chatting: real-time, text-based communication between individuals in what amounts to a temporary private chat room

IP Address: the numeric address of a computer on the internet; used to identify a computer and network in much the same way as a social security number or national identity number is used to identify a person

ISP: internet-service provider, a company that provides access to the internet for a fee; supplies customers with a software package, a username, a password, and telephone numbers to initiate a connection

IT: information technology, the broad subject concerned with all aspects of managing and processing information

Netizen: citizen of the internet; a person actively involved in the online community

Packet Sniffer: computer software or hardware that can intercept and log traffic passing over a network; often part of a firewall system; can be used to spy on users and collect sensitive information such as passwords

Secure Sockets Layer (SSL): a method developed for transmitting private documents and data over the internet; uses two-layer encryption to ensure security; most often used in websites that handle private data, such as credit-card or banking information; denoted by the use of "https" in the URL rather than the standard "http"

SMS/Text Messaging: short-message service; brief text messages of no more than a few hundred characters, sent electronically from one mobile phone to another

Social-Networking Site (SNS): a website that enables users to create public profiles and form relationships with the site's other users, e.g., Facebook, MySpace, Orkut

Uniform Resource Locator (URL): the global address of a document or page on the World Wide Web, e.g. http://www.freedomhouse.org/template.cfm?page=383&report=79&group=19 is the URL for *Freedom on the Net*

Universal Serial Bus (USB) Modem: a specific portable USB device that looks similar to a USB flash drive (a data storage device) and can be plugged into any USB port on a computer to allow broadband access to the internet

Value-added Network Service (VANS): a network provider hired to facilitate electronic data interchange or provide other network services; before the arrival of the World Wide Web, some companies formed value-added networks to exchange data with other companies, but contemporary VANS providers focus on offering data translation, encryption, secure e-mail, management reporting, and other services for their customers

Video Sharing: the practice of uploading video clips—including those captured using mobile phones with video features—for viewing by others; some video sharing takes place via paid web-hosting sites, but most occurs on popular free websites such as YouTube

Virtual Private Network (VPN): a way to maintain fast, secure, and reliable communication by using the internet to connect remote sites or users; often explained as tunneling a smaller network through a larger network, a VPN can be established to circumvent strict internet controls and censorship within a given country; multinational corporations that operate in repressive internet environments often purchase from the government the right to use VPNs to connect to their home offices

VoIP: Voice over Internet Protocol, a category of hardware and software that enables users to make telephone calls via the internet; these calls do not incur a surcharge beyond what the user is paying for internet access, just as users do not pay for sending individual e-mails

Web 2.0: the metaphorical second generation of the World Wide Web; refers to advanced graphical features, multimedia formats, greater interactivity and content production by users, and related online services, including blog hosting, video sharing, and social networking

Wi-Fi: wireless technology that provides an internet or network connection for properly equipped computers, mobile phones, and other such devices within a given physical or geographical area

Survey Team

Contributing Authors

Yaman Akdeniz is an associate professor at the CyberLaw Research Unit, School of Law, University of Leeds (UK) where he teaches and writes mainly about internet related legal and policy issues. He is also the founder and director of Cyber-Rights & Cyber-Liberties, a non-profit civil liberties organization. He has acted as an expert to the United Nations High Commissioner for Human Rights (UNHCHR) and published extensively on topics related to policing the internet. He is a graduate of the University of Leeds (PhD). He served as the analyst for Turkey and the United Kingdom.

Raman Jit Singh Chima is currently completing a degree in Arts and Law from the National Law School of India University, Bangalore. He has clerked for the Honorable Justice V.S. Sirpurkar of the Supreme Court of India, and is Chief Editor of the Indian Journal of Law and Technology. He was a Sarai-CSDS Independent Research Fellow in 2007, examining the regulation of the Internet by the Indian state. He served as the analyst for India.

Ming Kuok Lim is an advanced doctoral student in the College of Communications at Penn State University. His research focuses on the relationship between the use of new media, such as blogging, and the development of democracy. He has conducted a series of interviews with prominent bloggers in Malaysia and has served as an analyst for *Freedom in the World* for Singapore and Malaysia. He served as the analyst for Malaysia.

Mariam Memarsadeghi advises human rights and democracy promotion organizations internationally and is an outspoken advocate for women's rights and civil liberties in Islamic contexts. She is an expert on free media, internet freedom and internet initiatives for repressive regime contexts and founded the bi-lingual web magazine *Gozaar: A Journal on Democracy and Human Rights in Iran* while serving as Senior Program Manager at Freedom House. She has studied political science and political theory at Dickinson College (BA) and the University of Massachusetts, Amherst (MA) and is fluent in English and her native Persian. She served as the analyst for Iran.

Ory Okolloh is a lawyer, a political activist and blogger. She is the co-founder of Mzalendo, a website that tracks the performance of Kenyan Members of Parliament, and the co-founder of Ushahidi. She is a frequent speaker at conferences including TED Global and Poptech on issues around citizen journalism, the role of technology in Africa, and the role of young people in reshaping the future of Africa. Ms. Okolloh graduated summa cum laude with a B.A. degree in Political Science from the University of Pittsburgh, and graduated with a J.D. from Harvard Law School. She also writes one of the most popular blogs in the Kenyan sphere at Kenyan Pundit. She served as the analyst for Kenya and South Africa.

Giorgi (Giga) Paitchadze is the founder of the Georgian NGO New Media Institute, a veteran blogger, and political analyst. He has served as a trainer and educator in blogging and new media and as the organizer of the Caucasus BarCamp – a weekend retreat and educational training camp for bloggers from the Caucasus region. He is also the founder of Georgia's first social networking site, face.ge. He holds a postgraduate degree in International Relations and International Law (LL.M.). He served as the analyst for Georgia.

Carolina Rossini is a Fellow at the Berkman Center at Harvard University and also coordinates a project on policy for Open Educational Resources in Brazil with the Open Society institute. She holds positions at the Diplo Foundation as a fellow for the Internet Governance Program and at IQSensato as a Research Associate for the Access to Knowledge and Innovation Program. She is a Brazilian lawyer and a law lecturer, and was part of Brazilian Creative Commons team at Fundacao Getulio Vargas Law School, where she coordinated the Legal Clinical Program and the CC Latin America chapter of the Open Business project. Before moving to academic life, Ms. Rossini acted as in-house counsel for the Telefonica Telecommunications Group in Brazil focus in internet and telecom services. She served as the analyst for Brazil.

Alexey Sidorenko received his MA in Geography from Moscow State University and is currently based at Warsaw University. He is working on both a PhD in geography at Moscow and an MA in cultural studies at Warsaw. Both dissertations are dedicated to the juncture of politics, ICT and regional studies on the post soviet space. He worked for three years in Moscow for the Carnegie Centre, as a research assistant for the projects "Society and Regions" and "Russian Domestic Politics and Political Institutions". He is interested in electoral geography, cybergeography and in the internet and political representation in Russia, Eastern Europe, Caucasus and Central Asia. He served as the analyst for Russia.

Linnar Viik is an Estonian information society and innovation analyst and lecturer. He has worked part-time as Adviser to the Prime Minister of Estonia on Information Technology and Research & Development, and as the Head of the Secretariat of the Research and Development Council of the Government of Estonia and is also Member of Estonian Research and Development Council and Information Society Board. He received degrees in IT management and international economics at Tallinn Technical University and the University of Helsinki. He has published over 150 articles and research papers. He served as the analyst for Estonia.

The analysts for the reports on China, Cuba, Egypt and Tunisia are independent internet researchers who have requested to remain anonymous.

Ratings Review Advisers

Jon B. Alterman is director of the Middle East Program at the Center for Strategic and International Studies in Washington, D.C. He received his PhD in history from Harvard University, and he has worked on the personal staff of Senator Daniel Patrick Moynihan and on the policy-planning staff at the U.S. Department of State. He is the author of *New Media, New Politics?: From Satellite Television to the Internet in the Arab World.*

David Banisar is Director of the Freedom of Information Project of Privacy International in London. He is also a Non-Resident Fellow at the Center for Internet and Society at Stanford Law School and a Visiting Research Fellow at the School of Law, University of Leeds. Previously he was a Research Fellow at Information Infrastructure Project at the Kennedy School of Government at Harvard University and a co-founder and Policy Director of the Electronic Privacy Information Center in Washington, DC. He has worked in the field of information policy for seventeen years and is the author of books, studies, and articles on freedom of information, freedom of expression, media policy, whistleblowing, communications security, and privacy.

Guy Berger is head of the School of Journalism & Media Studies at Rhodes University, Grahamstown, South Africa. He is editor of the book *Media Legislation in Africa* (2007), published by UNESCO, and was keynote speaker at a UNESCO conference on Press Freedom and New Media in the same year. In 1995, he founded the Rhodes school's New Media Lab which in turn initiated what has become the world's largest annual gathering of African journalists. In 2008, Berger also raised R8m from the Knight Foundation and MTN towards research into the articulation of cell phones and the media industry. He writes a fortnightly media column for South Africa's leading independent newspaper.

Floriana Fossato has studied Russian literature, politics and society in Italy, Moscow and at University College London and lived and worked in Russia for more than a decade. She was a research associate at the Reuters Institute for the Study of Journalism at Oxford University for the project The Web That Failed: How opposition politics and independent initiatives are failing on the Internet in Russia. Beginning in 2009 she will be involved in a EU funded project on Media in Armenia, Azerbaijan and Georgia.

Shanthi Kalathil is an expert on media, civil society, and democratization. She is currently acting as a consultant to the Communication for Governance and Accountability Program (CommGAP) at the World Bank, a new initiative that seeks to explore the role of the public sphere—incorporating plural and independent media systems, the free flow of information, and free debate and discussion—in securing good governance and accountability. She was formerly a senior democracy fellow based in the Office of Democracy and Governance at the U.S. Agency for International Development, where she provided policy and programmatic advice on issues relating to civil society, media, and the Near East/Asia region, and an associate at the Carnegie Endowment for International Peace, where she co-authored *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule*, a widely cited, reviewed and translated volume on the political effect of the internet. She holds a B.A. from the University of California at Berkeley and an M.Sc. from the London School of Economics and Political Science, and is fluent in Mandarin.

Daniel Kimmage received his undergraduate education at the State University of New York at Binghamton and earned an M.A. in Russian and Islamic history from Cornell University. From 1997-2001, Kimmage lived in St. Petersburg, Russia, where he was the English-language editor of the quarterly journal *Manuscripta Orientalia* at the Institute of Oriental Studies. From 2003 to 2008, Kimmage was a regional analyst at Radio Free Europe/Radio Liberty, where he focused on politics, business, and media issues in Central Asia and Russia. His work has appeared in *The New York Times, The New Republic, Foreign Policy* and *Slate*. He is currently an independent consultant based in Washington, DC.

Sudhir Krishnaswamy is an Assistant Professor at the National Law School of India University. He graduated from the National Law School Bangalore in 1998 and went on to complete the Bachelor in Civil Law and the Doctorate in Philosophy of Law at Oxford University at the University of Oxford on a Rhodes scholarship. His research interests include constitutional and administrative law, property and intellectual property law, legal theory and the reform of legal systems. He is the Chief Editor of the *International Journal of Communications Law and Policy* and was an editor of the *Oxford University Commonwealth Law Journal*.

Xiao Qiang is the Director of China Internet Project and an adjunct professor at the Graduate School of Journalism, University of California, Berkeley. He is the Founder and Editor-in-Chief of

China Digital Times, a bi-lingual China news website. A theoretical physicist by training, he studied at the University of Science and Technology of China and entered the PhD program (1986-1989) in astrophysics at the University of Notre Dame. He became a full time human rights activist after the Tiananmen Square protests of 1989. He was the Executive Director of the New York-based NGO Human Rights in China from 1991 to 2002 and vice-chairman of the steering committee of the World Movement for Democracy. He is a recipient of the MacArthur Fellowship in 2001, and is profiled in the book *Soul Purpose: 40 People Who Are Changing the World for the Better*. He researches and writes about state online censorship and propaganda, emerging "Citizen Blogging" movement, and network activism in Chinese cyberspace.

Katitza Rodríguez is the Director of EPIC´s International Privacy Project and Coordinator of The Public Voice Coalition where she concentrates on comparative policy and legal aspects of privacy and data protection and is in charge of liaising with data protection authorities, policymakers, consumer and civil society organizations around the world. She is also Research Director for the "Privacy and Human Rights Report (PHR) 2008," (forthcoming) the most comprehensive survey of privacy laws and developments in the world. She was responsible for facilitating the participation of Civil Society in the Organisation for Economic Co-operation and Development (OECD) Ministerial in Seoul, Korea as well as the organization of the OECD Civil Society Forum.

Bridget Welsh is associate professor in the Southeast Asia Studies Program at Johns Hopkins University-SAIS. Her primary research interest focuses on 20th century Southeast Asian politics. She is the former chair of the Malaysia, Singapore, Brunei Studies Group and the editor of *Reflections: The Mahathir Years* (Johns Hopkins University Press, 2004) and co-editor of *Legacy of Engagement in Southeast Asia* (Institute of Southeast Asian Studies, 2008). She is currently completing an analysis of Malaysian voting behavior and the electoral system during the last ten years and a project examining the local dynamics in elections. She received her PhD from the Department of Political Science at Columbia University, and her MA from Columbia University.

Expert Methodology Committee

Jon B. Alterman is director of the Middle East Program at the Center for Strategic and International Studies in Washington, D.C (see above for full bio).

Derrick Cogburn is an expert on global information and communication technology (ICT) policy and in the use of ICTs for socio-economic development. He is currently an assistant professor at the Syracuse University School of Information Studies and senior research associate at the Moynihan Institute of Global Affairs at the Maxwell School of Citizenship & Public Affairs. He also directs the Collaboratory on Technology Enhanced Learning Communities (Cotelco), an award-winning social science research collaboratory investigating the social and technical factors that influence geographically distributed collaborative knowledge work, particularly between developed and developing countries. Additionally, he is also a faculty affiliate with the Convergence Center, a member of the Internet Governance Project, and is a faculty member of the Syracuse University Africa Initiative.

Sarah Cook is an Asia researcher at Freedom House and Assistant Editor for the *Freedom on the Net* index. She has served as assistant to the editor of the 2008 *Freedom of the Press* index and analyst for both that publication and *Freedom in the World*. Her research has covered human rights and media

developments in East Asia, Indochina, and the Middle East, including recent fact-finding trips to Hong Kong and Taiwan. She has also been a country report author on China for a recent Freedom House publication on the status of freedom of association. Before joining Freedom House, she co-edited the English translation of *A China More Just*, a memoir by prominent rights attorney Gao Zhisheng, and was twice a delegate to the United Nations Human Rights Commission meeting in Geneva for an NGO working on religious freedom in China. She received a B.A. in International Relations from Pomona College and as a Marshall Scholar, completed Masters degrees in Middle East Politics and Public International Law at the School of Oriental and African Studies in London.

Robert Guerra is the Project Director of Freedom House's Global Internet Freedom Initiative. The initiative aims to analyze the state of internet freedom, to expand the use of anti-censorship technologies, to build support networks for citizens fighting against online repression and to focus greater international attention on the growing threats to users' rights. He is also one of the founding directors of Privaterra - an ongoing project of Tides Foundation Canada that works with nongovernmental organizations to assist them with issues of data privacy, secure communications, information security, Internet Governance and internet Freedom. He advises numerous non-profits, foundations and international organizations and is often invited to speak at events to share the challenges being faced by social justice organizations in regards to surveillance, censorship and privacy.

Leslie Harris is the President and CEO of the Center for Democracy & Technology where is responsible for the overall vision, direction and management of the organization and serves as the organization's chief spokesperson. Since joining CDT, she has been involved with a wide range of issues related to civil liberties and the internet, including, government data-mining for counterintelligence, government secrecy, privacy, global internet freedom, intellectual property, data security and internet censorship. She testifies before Congress on issues related to technology, the internet and civil liberties and writes, speaks on internet issues and is regular contributor to several online publications and blogs. She received her law degree from the Georgetown University Law Center and her BA at the University of North Carolina at Chapel Hill.

Shanthi Kalathil is a consultant to the Communication for Governance and Accountability Program (CommGAP) at the World Bank (see above for full bio).

Daniel Kimmage is currently an independent consultant based in Washington, DC and an expert in Russia and Central Asia (see above for full bio).

Karin Deutsch Karlekar is the managing editor of *Freedom of the Press*, an annual survey that tracks trends in media freedom worldwide and served as managing editor for *Freedom on the Net*. She coordinates the research, ratings, and editorial processes for the survey, and also writes a number of the country reports. In addition, she has conducted research and assessment missions to Nigeria, Afghanistan, Sri Lanka, and Pakistan, and has traveled extensively in Asia and Africa. She regularly serves as the spokesperson for Freedom House on media and press freedom issues, and has been quoted extensively in U.S. and foreign media outlets. For the past five years, she has represented Freedom House in the International Freedom of Expression Exchange (IFEX) network, and in February 2006 was elected as IFEX Convenor and head of IFEX's governing Council. Prior to joining Freedom House, Dr. Karlekar was a Deputy Editor for the electronic division for the Economist Intelligence Unit and also served as a consultant to Human Rights Watch. She holds a Ph.D. in Indian History from Cambridge University, England.

Christopher Walker is Director of Studies at Freedom House where he helps oversee a team of senior analysts and researchers in devising overall strategy for Freedom House's analytical publications. He is responsible for generating special studies and reports, conducting briefings, and responding to critical news and democracy issues through statements and op-eds. Before joining Freedom House, he worked at the EastWest Institute. He is also an Adjunct Assistant Professor of Global Affairs at New York University and has contributed to a wide range of publications. He received his undergraduate degree from Binghamton University, State University of New York, and Master's Degree from Columbia University's School of International and Public Affairs.

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

120 Wall Street, New York, NY 10005
(212) 514-8040

www.freedomhouse.org

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 governments 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.