Internet Filtering in 
Sub-Saharan Africa

Overview
Many sub-Saharan African governments view the Internet as a key tool for development and are developing ICT policies accordingly, though the region still lags behind the rest of the world in both number and percentage of Internet users. Sub-Saharan Africa has a history of media abuses and restrictions on freedom of the press, and the region would seem a likely setting for equally restrictive Internet policies. However, ONI testing found evidence of a technical filtering regime in only one country, Ethiopia. As the Internet continues to develop in sub-Saharan Africa, so too will laws regulating its use. To what extent these laws will encourage education, commerce and online governance or restrict free expression largely remains to be seen.

Internet in Sub-Saharan Africa
Internet access is more scarce in sub-Saharan Africa than anywhere else in the world. African Internet users account for less than 5 percent of the world’s online population, and many countries’ Internet penetration rates are less than 1 percent. This is likely to change in the near future, particularly with the growth of the mobile Internet and the rapid increase of mobile phone use in the region.

According to 2008 data from the International Telecommunications Union, only five sub-Saharan African countries had penetration rates exceeding 10 percent, four of which were small island nations. At 37.8 percent, the Seychelles have the highest penetration rate in all of sub-Saharan Africa; Sierra Leone has the lowest, at 0.2 percent. Nigeria, with 11 million Internet users, has the largest online population. Of the sub-Saharan African countries discussed in this profile, Zimbabwe (the one non-island nation to break the 10 percent threshold) has the highest penetration rate at 10.5 percent, followed by Uganda (7.8 percent) and Nigeria (7.26 percent). Ethiopia lags behind at 0.4 percent, the second-lowest rate on the continent.

Poor infrastructure is the major factor in the region’s low ICT adoption rates. Only 17 percent of sub-Saharan Africans have electricity access; in rural areas this drops to 5 percent. Areas that are connected to power grids often suffer outages, and power shortages have forced many countries to operate under load-shedding agreements, or rolling blackouts, in which residents receive electricity on a schedule that ranges from every other day to once a week or less. Many ISPs still obtain bandwidth from foreign service providers via satellite, which can be up to five times as expensive as bandwidth delivered via undersea cable. Though West and Southern Africa have connected to India via the South African Telecom-3 (SAT-3) submarine fiber optic cable for some time, until the arrival of Seacon in July 2009, Eastern Africa was excluded from the international cable system. Plans for the East African Submarine
Cable System (EASSy) have been repeatedly delayed. In 2006, massive inflation in Zimbabwe caused government-owned ISP TelOne to amass a USD700,000 debt to international satellite communications provider Intelsat. Intelsat cut service to the country for several weeks, causing severe delays for Internet users. Service was restored after the country’s reserve bank paid TelOne’s outstanding debt, but the incidence highlights the strain many sub-Saharan African ISPs face in obtaining adequate bandwidth for their customers.

In the 1990s many sub-Saharan African countries began to privatize their telecommunications industries in an attempt to boost the private sector and thereby attract greater foreign investment. Privatization has met with mixed success: in Niger, government plans to sell the national mobile phone network in multiple sections prompted a two-month strike by telecoms workers, who feared the industry would suffer from segmentation. In Uganda, where the telecoms market was opened to competitors in 1997, concerns about corruption in the privatization minister’s office led the country’s parliament to suspend all privatization operations during 1998. The sale of public telecoms companies in both Ghana and Zambia is being challenged in court at the time of writing; in both cases the national governments allegedly failed to follow proper privatization protocols. Still, privatization has helped many countries with flagging telecoms companies revitalize their telecoms industries, and in many cases privatization has marked the first step toward major ICT expansion.

Many sub-Saharan African governments, recognizing the potential of ICT to encourage development, have made serious efforts to expand Internet access in their countries. In April 2009, the government of Zimbabwe announced a plan to establish Internet cafés at post offices in rural areas. Rwanda’s 2006-2010 ICT plan, which covers education, governance, infrastructure, legislation and human capacity development, is aimed at helping the country “‘leapfrog’ into the digital-era global economy.” Uganda’s 2009/2010 government budget includes support for expanding current ICT infrastructure, linking most of the country’s major towns through 1500 km of optical fiber and providing for connectivity to ease the transition to the East African Submarine Cable System (EASSy), scheduled to be completed in June 2010. Ethiopia has also made attempts to increase available broadband by laying fiber optic cable along the country’s major highways, by making overtures to EASSy and by connecting Addis Ababa to existing fiber optic networks in Port Sudan and Djibouti. Nigeria is perhaps the most well established country in terms of ICT infrastructure – the country has its own communications satellite and is connected to India through the SAT-3 cable – and its National Information Technology Development Agency focuses on expanding Internet access to rural areas, supporting electronic governance, and increasing personal computer ownership.

Though most governments agree that greater use of ICT is beneficial for their citizens, sub-Saharan African countries vary vastly in the scope and availability of Internet services. Nigeria currently has more than 100 licensed ISPs, while Ethiopia continues to maintain strict control over its single, government-owned telecoms company. Many countries limit the provision of Voice Over Internet Protocol (VOIP) services to state-owned companies; others restrict its use entirely.
had opened VOIP to private companies.21 The adoption of WiMAX, which expands the reach of wireless access to 30 miles (compared with 300 feet for traditional WiFi) and is less expensive than DSL, has been a boon for rural access in the region; in 2007 the United Nations announced a plan to utilize WiMAX to increase connectivity in sub-Saharan Africa,22 and multiple companies have initiated WiMAX operations throughout the continent.23

In-home Internet access is still prohibitively expensive for most sub-Saharan African citizens; prices in Uganda can be as high as USD350 per month, or nearly one-third the GDP per capita.24 As a result, most sub-Saharan African Internet users get online at public Internet cafés, where access is generally slow and unreliable. Despite this obstacle, vibrant online communities exist in many countries: South Africa’s bloggers number in the thousands,25 and the number of Facebook users in Nigeria increased almost six-fold between July 2008 and July 2009.26

Legal and Regulatory Framework
The last decade has seen a push for greater ICT regulation in sub-Saharan Africa; many countries are enacting new legislation to address ICT ownership, provision and use. Existing media law has also been applied to online content and activity.

Though many sub-Saharan African constitutions guarantee freedom of expression and of the press, many governments use laws against defamation and laws protecting national security to curtail these freedoms. Ethiopia’s Mass Media and Freedom of Information Proclamation of 2008 increases fines for journalists convicted of defamation, allows the government to close any publication considered a threat to national security, and does nothing to reduce the overbearing powers of the Ministry of Information, which has the authority to issue or deny press licenses, monitor the media and manage the Ethiopian News Agency.27 Zimbabwe’s 2002 press law gives the country’s Media and Information Commission the power to control the licensing of journalists,28 and the commission has exercised this power to prevent reporting on elections and to bar foreign journalists from entering the country.29 Uganda’s Media Centre has similarly refused to accredit foreign journalists and those who write critically of the ruling party.30 Malawi prohibits the publication or transmission of anything “that could be useful to the enemy,” as well as religiously offensive and obscene material.31 Until the passage of a new press law in 2005, Burundi required a government censor to review all news articles four days before publication.32

Many sub-Saharan African countries have recently developed or are currently developing legislation addressing cybercrime and online security. Uganda introduced three bills in 2004, still under review at the time of writing, to regulate online activity. If passed, they will impose penalties of up to seven years in prison and/or UGX3.36 million (approximately USD1600) for those convicted of malicious or unauthorized used of a computer, including using a computer to access or distribute child pornography, with harsher penalties imposed for crimes committed on “protected” computers, defined as those used in connection with matters of national security, criminal law, public infrastructure, banking, or public safety.33

Nigeria’s Computer Security and Critical Information Infrastructure Protection Bill, proposed in 2005, requires ISPs to retain user data and make it available to law enforcement. The bill may also serve as gateway to more extensive
filtering or Internet controls. As of 2008, the bill was still undergoing debate and revisions. 

Zambia’s cybercrime law was developed partly in response to a case in which someone hacked into the State House Web site and replaced the president’s official photograph with a cartoon. The charges were dropped because Zambia lacked appropriate cybercrime laws at the time. In 2004, Zambia enacted cybercrime legislation that provides for penalties of up to 25 years in prison for those convicted of hacking, electronic fraud and other online crimes.

Mauritius’ Computer Misuse and Cybercrime Act 2003 imposes penalties of up to 20 years in prison and fines of MUR200,000 (USD6201) for convicted hackers; anyone who reveals a password “or any other means of gaining access to any program or data held in any computer system...knowing that it is likely to cause prejudice to any person” can be fined MUR50,000 (USD1550) and sentenced to 5 years in prison.

Regional efforts to combat cybercrime also exist: the East African Community (consisting of Kenya, Tanzania, and Uganda) and the South African Development Community (consisting of Malawi, Mozambique, South Africa, Zambia, and Zimbabwe) have both enacted plans to standardize cybercrime laws throughout their regions.

Laws regulating obscenity also restrict online content. In 2006, the government of South Africa began prohibiting sites hosted in the country from displaying X18 (explicitly sexual) and XX content (including child pornography and depictions of violent sexual acts); site owners who refuse to comply are punishable under the Film and Publications Act 1996. In other countries, such as Botswana, older obscenity laws may or may not apply online: though the Telecommunications Act 1996 forbids transmitting “indecent, obscene or menacing” content, the country’s 2004 National ICT Policy notes, “Current legislation dealing with pornography or undesirable content may not be adequate to cover such matters as ‘exporting’ child pornography through the Internet.” Many sub-Saharan African countries, including Lesotho, Malawi, and Zambia, regulate obscene content to some degree. As Internet usage grows in these countries, observers can expect to see these laws re-examined and possibly revised with respect to online content.

Laws governing ICT provision have an immense impact on Internet use in some countries. In Ethiopia, the government restricts the provision of Internet access to the state-owned Ethiopian Telecommunications Corporation (ETC) and the Ethiopian Telecommunication Agency (ETA). The ETA grants the ETC a monopoly license as Ethiopia’s sole ISP and seller of domain names under the country code top-level domain, “.et.” Internet cafés and other resellers of Internet services must be licensed by the ETA and must purchase their access through the ETC. Individual purchasers must also apply for Internet connections through the ETC. Though Ethiopia has considered some limited privatization of the telecommunications market, these plans are on hold until at least 2010 despite acknowledgments that the ETC has not been an effective service provider. Countries with small online populations, such as Burkina Faso, Central African Republic, Mauritius and Niger, tend to have de facto monopolies, often run by formerly state-owned service providers.
Surveillance
Zimbabwe has one of sub-Saharan Africa’s most extensive surveillance regimes. The Post and Telecommunications Act of 2000 allows the government to monitor e-mail usage and requires ISPs to supply information to government officials when requested. Though the Supreme Court ruled in 2004 that sections of the law violated the constitution, the government has subverted the ruling by requiring ISPs to sign contracts with government-owned telecommunications company TelOne stipulating that they report any e-mail with “offensive or dangerous” content. Zimbabwe strengthened its Internet surveillance policies with the Interception of Communications Bill of 2006, which established a telecommunications agency called the Monitoring and Interception of Communications Center to oversee, among other things, all telecommunications and postal services. Telecommunications and Internet service providers are required to ensure that their systems are technically capable of monitoring and to cover all associated costs. According to Reporters Without Borders, during the 2008 presidential elections, government forces hacked into journalists’ e-mail accounts; eight journalists were fired for allegedly failing to support President Robert Mugabe and the ruling party.

In late December 2006, the government-run Ethiopian Telecommunication Agency, Ethiopia’s sole ISP, began requiring Internet cafés to log the names and addresses of individual customers, apparently as part of an effort to track users who engaged in illegal activities online. The lists are to be turned over to the police, and Internet café owners who fail to register users face prison.

The initial draft of Uganda’s Interception of Communications Bill of 2007 allowed phone tapping and other forms of electronic surveillance on people suspected of committing terrorism or crimes against the State without requiring a court order. The bill drew ire from Ugandan lawyers, human rights organizations and citizens, who criticized the bill for subverting the courts and giving power directly to security agents. In May 2009, the bill was altered, giving Uganda’s High Court, rather than the security minister, the power to issue the surveillance warrant. The change made the bill more likely to be approved, but some provisions in the bill – such as allowing security agents to intercept and open suspects’ mail – directly contradict pre-existing laws that protect privacy, such as the Communications Act of 1997. Communications acts in both Ghana and Nigeria also threaten Internet users’ privacy. Ghana’s Telecommunications Act 2005 gives the president the power to order ISPs to monitor online communications and hand over user data to the authorities. In Nigeria, the Communications Act 2003 gives the Commission the authority to require “any person who is subject to [the] act” to give the Commission any information “including but not limited to accounts and records or any document that is relevant to the exercise of the Commission’s powers and functions under this Act” for the purposes of national security. Punishment for refusal includes a year in prison and a fine of NGN100,000 (USD676).

The events of September 11, 2001 have led governments around the world to develop new anti-terrorism legislation; sub-Saharan Africa is no exception. These laws often grant governments expansive surveillance privileges and reduce citizens’ right to privacy. Kenya’s 2003
Suppression of Terrorism Bill prohibited “collect[ing],” “mak[ing]” or “transmit[ting]” information that may be helpful to terrorist organizations, including online information. The bill prompted such an outrage among Kenyan citizens, many of whom worried about how the government’s planned to define what constituted “helpful” information, that the Kenyan parliament eventually rejected it. However, anti-terrorism bills in countries ranging from South Africa to Tanzania have increased governments’ ability to conduct surveillance for loosely defined national security purposes.

Internet Filtering in sub-Saharan Africa
The first recorded case of Internet censorship in sub-Saharan Africa occurred in Zambia in 1996. The Zambian government, angered by a newspaper article containing information on then-secret plans to hold a referendum on the country’s 1996 constitution, made possession of the offending newspaper edition a criminal offense. They extended their prosecution to the Internet, threatening Zambian ISP Zamnet with criminal charges if the ISP did not take the edition offline.

In most of sub-Saharan Africa, the technical approach to Internet filtering has not changed much since 1996. Sporadic IP blocking of sites, rather than more sophisticated URL blocking, is the norm, and most filtering targets political content. However, many countries in the region also practice more indirect forms of censorship such as arresting or threatening bloggers, online journalists, and other Internet users. In June 2009 a Tanzanian blogger was arrested for altered photographs of the president; Zimbabwean authorities arresting a 60-year-old blogger in 2007 for allegedly practicing journalism without accreditation. Gambia is a particularly egregious offender of the right to freedom of expression: in 2007 a Gambian journalist living in the US was convicted of sedition for an article published online; she was fined USD12,000; in 2006 the Gambian police ordered all subscribers to an online independent newspaper to report to the police or face arrest. Bloggers and online journalists have also been arrested in Nigeria, South Africa, and Mauritania. Raids on Internet cafés are another form of intimidation: security agents in Eritrea raided an Internet café and arrested three customers on unspecified charges in December 2008; in 2005, Zimbabwean authorities arrested 40 people in a raid on a local Internet café because an e-mail insulting Mugabe was sent from the location. This type of indirect censorship can be difficult to measure, and its effects may reach deep into sub-Saharan African online communities, causing Internet users to self-censor or avoid attempting to access sensitive content out of fear of government retribution.

ONI tested for the presence of technical Internet filtering in four sub-Saharan African countries in 2008-2009: Ethiopia, Nigeria, Uganda, and Zimbabwe. Despite government attempts in all four countries to control information, only Ethiopia was found to be filtering the Internet. Ethiopia’s filtering regime targets independent media, blogs, and political reform and human rights sites, though the filtering is inconsistent: many prominent sites that are critical of the Ethiopian government remain accessible, while some blocked sites seem harmless. All blogs hosted at blogspot.com and nazret.com, a site the aggregates Ethiopian content, are blocked. The sites of opposition political parties, minority ethnic groups, independent news organizations and Ethiopia-specific human
rights organizations appeared to be a priority for blocking, though many international sites containing comparable information (such as CNN, Voice of America, Human Rights Watch and Amnesty International) were not blocked.

In March 2009, Ethiopia unblocked a number of Web sites supporting political reform, including the Committee to Protect Journalists, in what may have been a reaction to the February 2009 release of a United States Department of State report on human rights in the country.\(^7^0\)

ONI testing in other countries revealed no evidence of filtering. ONI found that six ISPs in Nigeria all appear to be allowing unrestricted access to the Internet. These results concur with testing conducted near the 2007 elections, during which ONI concluded that no filtering took place.\(^7^1\) In Zimbabwe, despite severe press restrictions and pervasive surveillance of online communications, ONI found that the government has not yet implemented an Internet filtering regime.

In Uganda, ONI testing revealed no evidence of filtering. However, though the government does not actively filter the Internet, it temporarily blocked the site of an independent radio station during the 2006 presidential elections, blocking access to over 600 unrelated sites in the process.\(^7^2\) It is not unreasonable to believe that similar incidents may occur in the upcoming 2011 elections.

**Conclusion**
The absence of widespread filtering in sub-Saharan Africa does not indicate that these countries are taking an intentionally open approach to the Internet. The growth of the Internet in sub-Saharan Africa has had undeniably positive effects for the region’s countries and citizens, and increased filtering would likely temper these effects. However, the direction Internet regulation will take in the region remains to be seen.

*Author: Rebekah Heacock*
NOTES


st-facebook-usage-statistics-by.html.

Nigerian Facebook users increased from 99,720 in July 2008 to 569,180 in July 2009.


48 Ibid.


