ICT Policies Relating to Privacy, Freedom of Expression and Access to Information: A Briefing Paper*

David Banisar**

***Prepared for the International Workshop on *The Nexus Between ICTs and Human Rights in Africa* organized by Human Rights and Peace Centre, Faculty of Law, Makerere University, Uganda with assistance from the International Development Research Centre, Ottawa, Canada**

****Privacy International**

I. Introduction

This document is a brief primer to some of the key issues in three areas: privacy, freedom of expression and access to information, and how they relate in ICT policy.

While all the areas have existed as their own independent (and sometime overlapping and conflicting) areas of policy, they have all undergone significant changes with the evolution in the last twenty years of ICTs. The changes have been both positive and negative. ICTs have made access to information and freedom of expression easier for those who have less resources and expanded the ability for mass distribution. At the same time, ICTs allow for automated censorship and pose new threats to privacy that did not exist before.

II. Privacy

1. Overview - Defining Privacy and African Recognition

Privacy is a broad concept relating to the protection of individual autonomy and the relationship between an individual and society, including governments, companies and other individuals. It is considered a keystone right that is essential to protecting individual's ability to develop ideas and personal relationships. It can be divided into the following separate but related concepts:

- **Information privacy** – the right of individuals to control personal information such as financial and medical information held by other parties and the creation of rules governing the collection and handling of this information. It is also known as "data protection";

- **Bodily privacy** - the protection of people's physical selves against invasive procedures such as genetic tests, drug testing and cavity searches;

- **Communications privacy** - the privacy of communications made using postal mail, telephones, e-mail and other forms; and

- **Territorial privacy** - the setting of limits on intrusion into the domestic and other environments such as the workplace or public space. This includes searches, video surveillance and ID checks.

The right to privacy is recognized in most international human rights treaties including the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the European Convention on Human Rights, the American Declaration of the Rights and Duties of Man, and the American Convention on Human Rights.

The African Charter on Human and People's Rights does not include any specific rights of privacy. However the AU Declaration on Freedom of Expression and Information interprets Article 9 on freedom of expression to give individuals a right of access to their own records, which is also a recognized privacy right:

> Everyone has the right to access and update or otherwise correct their personal information, whether it is held by public or by private bodies.

Other instruments such as the African Charter on the Rights and Welfare of the Child do specifically recognize the right of privacy. Article 10 on Protection of Privacy states:

> No child shall be subject to arbitrary or unlawful interference with his privacy, family home or correspondence, or to the attacks upon his honour or reputation, provided that parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children. The child has the right to the protection of the law against such interference or attacks.

The 2004 Arab Charter on Human Rights, which has also been signed by a number of African states in North Africa, also recognizes privacy. Article 21 states:

> (1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour or his reputation.
> (2) Everyone has the right to the protection of the law against such interference or attacks.

In October 2008, the Economic Community of West African States (ECOWAS) reported that its telecommunications ministers had agreed to an agreement on personal data protection.[1] According to ECOWAS, the text "aims at filling the legal gap relating to personal data protection. It is also projected at establishing in each Member State a mechanism against privacy through personal data collection, processing, transmission, storage and use."

2. Information Privacy and ICTs

Of the four aspects listed above, the most important privacy area involving ICTs is information privacy. As stated above, this relates to the controls on the collection and use of personal information. This could cover a number of different technologies and issues including government databases relating to tax, medical, employment, criminal records and citizenship; technologies for identification including identity card systems, fingerprints, and DNA; and mandatory medical testing for employment, such as for HIV.

Over the past 40 years, concerns over information being collected in computer databases and its misuse led to the creation of rules known as fair information practices on the collection, handling, and use of personal information.[2] The basic fair information practices are:

- **Accountability**: An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

- **Identifying Purposes**: The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

- **Consent**: The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate.

---

[1] ECOWAS, ECOWAS TELECOMMUNICATIONS MINISTERS ADOPT TEXTS ON CYBER CRIME, PERSONAL DATA PROTECTION, Press Release N°: 100/2008, 16 October 2008.

[2] The principles were first proposed by the US Department of Health, Education and Welfare in 1974 and adopted into law in numerous countries.

- **Limiting Collection**: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

- **Limiting Use, Disclosure, and Retention**: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

- **Accuracy**: Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

- **Safeguards**: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

- **Openness**: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

- **Individual Access**: Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

- **Challenging Compliance**: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.[3]

3. Legal Protections

Most constitutions in African states have some reference to protection of privacy including a right of privacy for family, domicile or communications. Section 37 of the 1999 Constitution of the Federal Republic of Nigeria states that "The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected." Some go further and provide for extended rights. For example, the Constitution of Cape Verde includes those rights and includes detailed rights of data protection and access:

> **Article 44: Utilisation of computerised means and protection of personal data**
>
> **1.** All citizens have the right of access to computerised data concerning them, and shall have the right to demand their rectification and updating, as well as the right to be informed of the purpose for which these are intended, as provided by the law.

---

[3] Canadian Standards Association Model Code for the Protection of Personal Information (Q830). Incorporated into Bill C-6, Personal Information Protection and Electronic Documents Act. http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/C-6_cover-E.html . See European Committee for Standardization, Data Protection and Privacy: The Initiative for Privacy Standardization in Europe, available at http://www.cenorm.be/isss/Projects/DataProtection/dp.default.htm

2. Utilisation of computerised means to register and handle a individually identifiable data regarding political, philosophical or ideological conviction, religious faith, party or union affiliation or private life shall be prohibited except:

(a) upon express consent of the person in question;
(b) upon authorisation as provided by law, with guarantees of non-discrimination;

when it is intended for the processing of statistical data not individually identifiable.

3. The law shall regulate the protection of personal data in computerised registers, conditions of access to databases, establishment and utilisation by public authorities and private entities of such databases or computerised support thereof.

4. Access to archives, files, computer records or databases for information of personal data related to a third party, shall not be allowed, as well as the transfer of personal data from one computer file to another belonging to different services or institutions, except in cases provided by law or judicial decision.

5. Under no circumstances may it a single national number be attributed to citizens.

6. Everyone shall be guaranteed access to information networks for public use, and the law shall define the system applicable to the flow of data across borders and the types of protection of personal data and other whose safeguard is justified by reasons of public interest, as well as the system of limitation of access, for purposes of defending the juridical values protected by the provisions of paragraph 4 or article 47.

7. Personal data contained in manual files shall be granted protection similar to that specified in the previous paragraphs, as provided by law.

Article 45: *Habeas data*

1. Every citizen shall be granted *habeas data* to ensure knowledge of information contained in computer files, archives or records and which related to him or her, as well as the right to be informed of their purpose and to demand the rectification or updating of the data.

2. The process of *habeas data* shall be regulated by law.

In over 50 countries around the world, governments have adopted comprehensive data protection acts based on the fair information practices. To date, only two countries in Africa, Tunisia and Mauritius, have adopted laws similar to these. In Zimbabwe, the Access to Information and Protection of Privacy Act (AIPPA), which the government has said is based on Canadian privacy laws, sets some legal standards for protection of privacy which seem to be completely unimplemented. In South Africa, the Law Reform Commission has proposed a comprehensive data protection act similar to those found in Europe. The governments of Tanzania and Kenya have also began discussions on the subject.

4. Communications Privacy

As mentioned above, the right of private communications is widely recognized around the world as an aspect of the right of privacy in documents such as the UN Declaration on Human Rights, the European Convention on Human Rights and national constitutions. These instruments require that any interference with communications must be legally justified and limited in scope.

Nearly all countries around the world have enacted laws or procedures on the interception of oral, telephone, fax and telex communications. In most democratic countries, intercepts are initiated by law enforcement or intelligence agencies only after it has been approved by a judge or some other kind of independent magistrate or high level official and generally only for serious crimes. Frequently, it must be shown that other types of investigation were attempted and were not successful. There is some divergence on what constitutes a "serious crime," and appropriate approval.

However, in practice, there are still considerable problems. A brief review of international surveys of human rights practices such as those produced by Human Rights Watch or the US State Department, find that the controls are inadequate in many countries. Opposition leaders, journalists and civil activists are frequent targets.

The development of ICTs has significantly changed the nature of telecommunications networks for voice communications. The simple analog switches are increasingly being replaced with sophisticated digital switches, digital mobile communications, satellite, voice-over-IP (VOIP) and other technologies. As new telecommunications technologies emerge, many countries are adapting existing surveillance laws to address the interception of networked and mobile communications. These updated laws pose new threats to privacy in many countries because the governments often simply apply old standards to new technologies without analyzing how the technology has changed the nature and sensitivity of the information. For example, a senior Vodafone official revealed in February 2009 that the company provided communications data to the Egyptian government in March 2008 to identify who was protesting food price raises.[4]

The first is to promote laws that make it mandatory for all companies that develop digital telephone switches, cellular and satellite phones and all developing communication technologies to build in surveillance capabilities. This can be to facilitate the continued interception of communications. In South Africa, the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 (the Interception Act) adopted in 2002 requires that all telecommunications services, including Internet Service Providers, make their services capable of being intercepted before they could offer them to the public. It also sets detailed requirements for identification of mobile users and there has been extended discussions about requiring all foreigner register their mobile phones upon entry into the country. In Zimbabwe, the Interception of Communications Act

[4] Vodafone exec warns against tech regulation, ZDNet, 11 February 2009.

similarly requires providers to assist with interception.[5] A similar bill was recently introduced in Uganda.

Another issue is the increasing attempts by governments to seek limits on the use of products that provide encryption, a technique that allows people to scramble their communications and files to prevent others from reading them. Companies such as Research in Motion, have been required to limit their security systems in the Blackberry mobile devices to facilitate interception. In many other nations, users can be forced to disclose their encryption keys or face criminal sanctions.

A related effort for enhancing government control of the Internet and promoting surveillance is also being conducted in the name of preventing "cyber-crime," "information warfare" or protecting "critical infrastructures." Under these efforts, proposals to increase surveillance of the communications and activities of Internet users are being introduced as a way to prevent computer intruders from attacking systems and to stop other crimes such as intellectual property violations. These include the mass retention of personal data about users and their activities such as Internet sites visited and mobile phone location data. In Nigeria, the Cybercrime Bill proposed in 2005 will require all service providers (telephone and internet) to record all traffic and subscriber information for such period as specified by the President, and to release this information to any law enforcement agency on the production of a warrant. The Economic Community Of West African States (ECOWAS), East African Community (EAC) and countries including Algeria, Botswana, Gambia and Uganda are also considering cybercrime legislation.

III. Freedom of Expression

1. Overview

In the past few years, there has been significant growth in Internet use in Africa. Individuals have an unprecedented ability to exchange ideas and information that bypass the traditional media controls. Chat rooms and blogs among some of the technologies give regular people the ability to meet and discuss current topics in a way that had never been available before except in small rooms or under tight supervision. For example in Kenya, Internet forums were widely used to disseminate information about the disputed 2007 election that the mass media was prevented from discussing.

[5] Interception of Communications Bill, available at <http://www.parlzim.gov.zw/cms/Bills/InterceptBill.pdf>.

In an attempt to prevent these technologies from undermining their control, many governments have imposed existing restrictions on speech, or adopted new legal and technical measures on Internet use.

Questions about the nature of how electronic media should be treated in comparison to the traditional technologies have been hotly debated around the world. Should individuals bloggers be required to register in the same way that a major media organization does? Should they be subject to the same laws on editorial control. Rights of reply and civil and criminal liability?

A recent survey by Market Trends Research International in Nigeria found that "91% say it is important to have freedom of the media and 72% say they should have the right to read whatever is on the Internet". [6]

2. Legal Measures for Protection and Restriction

Freedom of expression is well recognized as a fundamental human right. The leading instrument is the 1948 UN Declaration of Human Rights. Article 19 states:

> 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 and regardless of frontiers.

This recognition of the importance of the right is echoed in regional instruments in Africa, Europe and the Americas. Article 9 of the African (Banjul) Charter on Human and Peoples' Rights states:

> 1. Every individual shall have the right to receive information.
> 2. Every individual shall have the right to express and disseminate his opinions within the law.

The right of freedom of expression is also found in nearly every national constitution in Africa. For example, the 1992 Constitution of Angola states:

> **Article 32**
>
> 1. Freedom of expression, assembly, demonstration and all other forms of expression shall be guaranteed.
> 2. The exercise of the rights set out in the foregoing clause shall be regulated by law.
> 3. Groupings whose aims or activities are contrary to the fundamental principles set out in Article 158 of the Constitutional Law and penal laws, and those that, even indirectly, pursue political objectives through organizations of a military, paramilitary or militarized character, secret organizations and those with racist, fascist or tribalist ideologies shall be prohibited.
>
> **Article 35**
>
> Freedom of the press shall be guaranteed and may not be subject to any censorship, especially political, ideological or artistic.

[6] World Public Opinion on Freedom of the Media, WORLDPUBLICOPINION.ORG, May 1, 2008.

> The manner of the exercise of freedom of the press and adequate provisions to prevent and punish any abuse thereof shall be regulated by law.

These legal protections are illusory in many countries. Existing laws on national security, public order, and public morality are being used to suppress speech. Often, they are used in ever harsher ways that used against the traditional media since the targets of arrests and raids are little known and powerless. In Egypt, in 1999, when Shohdy Surur published a poem by his late father, the highly-regarded Egyptian poet Naguib Surur on a US based website, he become "the first Arab Internet prisoner of conscience" and was forced to flee the country. In October 2002, a Cairo appeals court upheld his one year jail sentence for violating the law on distributing materials that corrupted public morals. Security forces have also attacked critics of the government, charging them with publishing "false news" under existing media laws and targeted gay bloggers, entrapping many and charging them with publishing obscene materials. More commonly, ISPs are ordered to remove material or web sites.

Many countries are also adopting new laws that specifically target the use of new technologies to public banned materials. In Kenya, the recently adopted Communications (Amendment) Bill, 2008 imposes new penalties for publishing material:

> **84D** Any person who publishes or transmits or causes to be published in electronic form, any material which is lascivious or appeals to the prurient interest and its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied therein, shall on conviction be liable to a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years, or both.[7]

Governments also try and maintain state control over the provision of access. This can include requirements on the registration and shutdown of unlicensed Internet cafes. In some countries, officials raid and seize equipment for providers that attempt to bypass official controls or provide easy access to those espousing unpopular views with officials. In Nigeria, ISPS and cybercafes were required in 2006 to register with the Economic and Financial Crimes Commission or face shutdown. All users are required to provide photo ID and biographical information.

There are also questions about what types of protections should online publications enjoy. In particular, should Internet users be allowed to post anonymously and should governments and other be able to force publications to disclose their sources. In Africa, nearly 20 countries have legal or Constitutional protections on protection of sources. None of them appear to directly apply to electronic publications such as blogs.

---

7 Kenya Communications (Amendment) Bill, 2008 <http://www.eastandard.net/downloads/kca_act_2008.pdf>

3. Technical Measures

Along with the legal measures, many governments are also pursuing technical measures to limit access to materials they deem unacceptable. Many of these are being built into the systems so that the users will not have any control over their use. These efforts are often supported by western technology companies.

A primary method of restriction is the use of software or hardware technologies to block access to sites. Depending on the size and use of the network, they can be installed at the central access points or gateways to the country in small countries which are often controlled by the state telecommunications provider. In larger networks, they can be placed at the ISP or provider level.

Much of the decision making on what is restricted is hidden and subject to seemingly arbitrary decision-making by officials. Sometimes the systems block entire web domains such as YouTube. In other systems, it can be based on specific pages or even keywords. Search engine results can be filtered.

The reasons for blocking are varied. Most common is material that is deemed to be of an improper sexual nature. This can include non-obscene materials relating to homosexuality or family planning. Equally common in less democratic states is materials that criticize the government. In Tunisia, access to social networking site FaceBook is intermittingly blocked. OpenNet reports that Ethiopia blocks many opposition websites.[8] Some indicate that a site is blocked while others make it appear falsely that a site is down or the page no longer exists.

The systems can also be used to block internal material. In Kenya, government servers block access by public servants to the Anti-Corruption Committee anti-corruption web site which allows for whistleblowers to report corruption information anonymously.[9]

In addition, the censorship is backed up with surveillance of users to punish them if the bypass the controls. This question also ties into the issue of communications privacy. Electronic records that telecommunications providers are being required to retain can also be used to identity sources of information. In South Africa, at the end of September 2005, the Mail and Guardian newspaper had a Section 205 subpoena directed at MWeb, its co-owner and host of its website, *M & G Online*, requiring the company to hand over electronic records relating to the online publication of an excerpt of an Imvume Management bank statement, as part of the "Oilgate" story.

IV Access to Information

1. Introduction

[8] Ethiopia blocks opposition Web sites – watchdog, Reuters, 01 May 2007.

[9] Kenya's Civil Servants Forbidden to Access Gov Whistleblowing Site?, OpenNet, 30 May 2008.

ICTs hold the promise of extending and promoting the right of access to information held by the government and other bodies. Information previously held in closed cabinets or remote libraries can now be available to everyone in an easy and inexpensive manner.

Access to information held by government bodies, also known as Freedom of Information, is widely recognized worldwide as an essential human right. It is an essential right for every person. It allows individuals and groups to protect their rights. It is an important guard against abuses, mismanagement and corruption. It can also be beneficial to governments themselves – openness and transparency in the decision-making process can improve citizen trust in government actions.

2. Legal rights to access

Access to information is widely recognized worldwide as an essential human right. There is a growing body of agreements, treaties, resolutions, guidelines and model bills adopted by international organizations promoting access to information as an international human right and as a key part of administrative law on issues such as environmental protection and anti-corruption.

At its first session in 1946, the General Assembly of the United Nations recognized that "Freedom of information is a fundamental human right and is the touchstone of all the freedoms to which the United Nations is consecrated." This was incorporated into the 1948 UN Declaration of Human Rights as Article 19 which states:

> 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 and regardless of frontiers.

Article 9 of the African Charter on Human and Peoples' Rights states that "Every individual shall have the right to receive information".[10] The Convention created the African Commission on Human and Peoples' Rights. In October 2002, the Commission adopted the Declaration of Principles on Freedom of Expression in Africa.[11] The Declaration calls on member states to recognize freedom of expression rights. Section IV on "Freedom of Information" states that information is being held by public bodies for the public and that they should have a right to obtain the information.

The right to know as enshrined in national constitutions has also become a common feature. 18 countries in African have adopted a constitutional provision giving citizens a right to access information. Typically, the rights give any citizen or person the right to demand information from government bodies.

---

[10] African Charter on Human and Peoples' Rights, Nairobi, Kenya, June 1981. http://www.africa-union.org/root/au/Documents/Treaties/Text/Banjul%20Charter.pdf

[11] Resolution on the Adoption of the Declaration of Principles on Freedom of Expression in Africa, African Commission on Human and Peoples' Rights, 32nd Session, 17 - 23 October 2002.

The South African Constitution has one of the most expansive rights in the world. It goes even further and gives individuals the right to demand information "that is held by another person and that is required for the exercise or protection of any rights."

The following elements are typically found in national ATI laws:

- a right of a individual, organization or legal entity to be able to demand information from public bodies without having to show a legal interest;
- a duty of the body to respond and provide the information. This includes mechanisms for handling requests and time limits for responding to requests;
- exemptions to allow the withholding certain categories of information. These typically require that some harm to the interest must be shown before it can be withheld. These include the protection of national security and international relations, personal privacy, commercial confidentiality, law enforcement and public order, information received in confidence, and internal discussions.
- internal appeals mechanisms for requestors to challenge withholding of information;
- external review of the withholding of information. This includes setting up an external body or referring cases to an existing ombudsman or the court system;
- requirement for government bodies to affirmatively publish some types of information about their structures, rules, and activities. This if often done using ICTs

Over 80 countries around the world have adopted laws based on these elements. The right of access has thus had limited recognition in African nations. To date, only four countries – South Africa, Uganda, Angola and Zimbabwe – have adopted laws that meet the above principles while another 18 or so are currently considering proposals or bills. Of the four that have adopted laws, there have been implementation problems in all of the countries and in Zimbabwe, the right of access is considered non-existent because of the onerous censorship provisions also found in the Act.

3. ICTs and ATI

One major area of possible improvement is the opening up of previously closed systems for citizen-government interaction. For the past decade, E-government has been promoted as a new way of providing a more efficient means of operating while providing for more responsive government. The most ambitious view of e-government is the development of tools and systems that allow for citizens to participate in governance. It can allow ordinary citizens regardless of geography to comment and interact on government proposals, providing the government with information and insights to develop policies based on a broader range of viewpoints.

However, electronic government requires information as a prerequisite. Without access to information, it is not possible to have e-government. As a recognition of this, many national RTI laws now impose a duty on government agencies to routinely release certain categories of information on their websites. In Poland, each public body must create an online Public Information Bureau which is the primary method of accessing information under the Law on Access to Public Information. In Turkey, the main ministries have been very active in using electronic networks to make

information available, including encouraging users to submit requests and obtain status updates about their requests online.

Many other laws also require that government departments affirmatively publish information. These include acts on public administration, consumer protection, environment, court practices and statistics. Many other types of records of interest to consumers and consumer groups can be made available.

4. Barriers

The most significant barrier is the inability of many individuals to be able to use electronic resources, due to lack of access or training. The digital divide is a significant problem in many African countries: the telecommunications networks are of poor quality due to the dominance of state telecommunications providers and privitization has not improved the situation; There are high fees for calls and broadband deployment has been limited; There is also generally a low penetration of computers in homes and low availability of public access to networks. Furthermore, much of the access is from the large cities and people in small towns and rural areas are even less likely to have access. Another large hurtle is the education or even willingness of individuals to use electronic services, especially those from older generations. Polls of countries around the world have found significant numbers of people who are unwilling to go online to use the services, even if offered training. Some of this is due to privacy and security concerns.

It is also necessary to ensure that the information is provided in such a way that it is easy to use and find. Care should be taken to ensure that files are not too large to preclude users using telephone-based systems are not prevented from viewing them, and that formats are commonly available.[12]

[12] See US Department of Health and Human Services, Research-based Wed Design and Usability Guidelines. http://usability.gov/pdfs/guidelines.html

V. Additional Resources

APC Africa ICT Policy Monitor
http://africa.rights.apc.org/

APC ICT Policy Handbook
http://rights.apc.org/handbook/

Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (eds), Access Denied: The Practice and Policy of Global Internet Filtering, MIT Press, 2008. http://opennet.net/accessdenied

Ecowas & EUMOA, Harmonisation of the Legal Framework Governing ICTs in West Africa, Proposed guidelines . Draft of legal texts 1.2
http://www.uneca.org/disd/events/2007/ecowas-legal-framework/content/Harmonising_Legal_Framework_ICTs_West_Africa-Cisse-en.pdf

EPIC and Privacy International, Privacy and Human Rights 2006
http://www.privacyinternational.org/phr

Freedom House, Freedom of the Press 2008
http://www.freedomhouse.org/template.cfm?page=362

Privacy International, Freedom of Information Around the World 2006
http://www.privacyinternational.org/foisurvey

Privacy International and GreenNet, Silenced: Censorship and Control of the Internet, 2003.
http://www.privacyinternational.org/silenced