OpenNet Initiative Internet Censorship Data

Questions regarding this data may be directed to contact@opennet.net or +1 (416) 946-8903. Last update: November 1 2011

The OpenNet Initiative (ONI) uses a simple technical methodology to verify Internet censorship. In order to identify and document internet filtering, ONI checks two lists of websites in each of the countries tested: a global list (constant for each country) and a local list (different for each country). The global list is comprised of internationally relevant websites with provocative or objectionable content in English. The local lists are designed individually for each country to document unique filtering and blocking behavior. In countries where Internet censorship has been reported, the local lists also include those sites that were alleged to have been blocked. These lists are samples and are not meant to be exhaustive.

A data collection software client designed to query these pre-defined lists of URLs is distributed to researchers within countries suspected of engaging in Internet censorship. The list of URLs is accessed simultaneously over HTTP both in the country suspected of Internet filtering and a country with no filtering regime (e.g., Canada). The data gathered from the country with no filtering is used as a control to compare the data from the country suspected of filtering. Additional diagnostic work is performed to separate normal connectivity errors from intentional tampering. Where appropriate, the tests are run from different national level Internet service provider connections in the country to capture the possible differences in blocking behavior across different ISPs and across multiple days and weeks to control for normal connectivity problems.

The ONI publishes results from these tests in country profiles (see http://opennet.net/country-profiles). Each country profile includes the summary results of the empirical testing for filtering. The technical filtering data alone, however, do not amount to a complete picture of Internet censorship and content regulation. A wide range of policies relating to media, speech, and expression also act to restrict expression on the Internet and online community formation. Legal and regulatory frameworks, including Internet law, the state of Internet access and infrastructure, the level of economic development, and the quality of governance institutions are central to determining which countries resort to filtering and how they choose to implement Internet content controls. A brief overview of each of these factors is included in the each of the country profiles. Together, these sections are intended to offer a concise, accurate, and unbiased overview of Internet filtering and content regulation.

Each country is given a score on a five-point. The scores reflect the observed level of filtering in each of four themes:

1. **Political**: This category is focused primarily on Web sites that express views in opposition to those of the current government. Content more broadly related to human rights, freedom of expression, minority rights, and religious movements is also considered here.

2. **Social**: This group covers material related to sexuality, gambling, and illegal drugs and alcohol, as well as other topics that may be socially sensitive or perceived as offensive.

3. **Conflict/security**: Content related to armed conflicts, border disputes, separatist movements, and militant groups is included in this category.

4. **Internet tools**: Web sites that provide e-mail, Internet hosting, search, translation, Voice-over Internet Protocol (VoIP) telephone service, and circumvention methods are grouped in this category.

The relative magnitude of filtering for each of the four themes is defined as follows:

1. **Pervasive filtering** (score of 4): Filtering that is characterized by both its depth—a blocking regime that blocks a large portion of the targeted content in a given category—and its breadth—a blocking regime that includes filtering in several categories in a given theme.

2. **Substantial filtering** (score of 3): Filtering that has either depth or breadth: either a number of categories are subject to a medium level of filtering or a low level of filtering is carried out across many categories.

3. **Selective filtering** (score of 2): Narrowly targeted filtering that blocks a small number of specific sites across a few categories or filtering that targets a single category or issue.

4. **Suspected filtering** (score of 1): Connectivity abnormalities are present that suggest the presence of filtering, although diagnostic work was unable to confirm conclusively that inaccessible websites are the result of deliberate tampering.

5. **No evidence of filtering** (score of 0): ONI testing did not uncover any evidence of websites being blocked.

Through examination of both technical and contextual data the ONI derives a measure (low, medium, or high) of the observed transparency and consistency of blocking patterns. The transparency score given to each country is a qualitative measure based on the level at which the country openly engages in filtering. In cases where filtering takes place without open acknowledgment, or where the practice of filtering is actively disguised to appear as network errors, the transparency score is low. In assigning the transparency score, we have also considered the presence of provisions to appeal or report instances of inappropriate blocking. Consistency measures the variation in filtering within a country across different ISPs—in some cases the availability of specific Web pages differs significantly depending on the ISP one uses to connect to the Internet.

About the OpenNet Initiative

The OpenNet Initiative is a collaborative partnership of three institutions: the Citizen Lab at the Munk School of Global Affairs, University of Toronto; the Berkman Center for Internet & Society at Harvard University; and the SecDev Group (Ottawa).

Our aim is to investigate, expose and analyze Internet filtering and surveillance practices in a credible and non-partisan fashion. We intend to uncover the potential pitfalls and unintended consequences of these practices, and thus help to inform better public policy and advocacy work in this area. To achieve these aims, the ONI employs a unique multi-disciplinary approach that includes:

- Development and deployment of a suite of technical enumeration tools and core methodologies for the study of Internet filtering and surveillance;

- Capacity-building among networks of local advocates and researchers

- Advanced studies exploring the consequences of current and future trends and trajectories in filtering and surveillance practices, and their implications for domestic and international law and governance regimes.

Reading and Resources

OpenNet Initiative http://opennet.net

Robert Faris and Nart Villeneuve, "Measuring Global Internet Filtering" in Ronald
Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, eds., *Access Denied:
The Practice and Policy of Global Internet Filtering*, (Cambridge: MIT Press)
2008. http://opennet.net/sites/opennet.net/files/Deibert_02_Ch01_005-028.pdf

Steven J. Murdoch and Ross Anderson, "Tools and Technology for Internet Filtering," in
Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, eds., *Access
Denied: The Practice and Policy of Global Internet Filtering*, (Cambridge: MIT
Press) 2008. http://opennet.net/sites/opennet.net/files/Deibert_04_Ch03_057-
072.pdf