OpenNet Initiative

Survey of Government Internet Filtering Practices Indicates Increasing Internet Censorship

First Year of Global Survey Examines 41 Countries by Political, Social and National Security Filtering

OXFORD, ENGLAND (May 18, 2007) – Twenty-five countries around the world out of 41 countries surveyed block or filter Internet content, indicating a global trend towards Internet censorship, according to the first year of a global survey of Internet filtering techniques by governments released today by the OpenNet Initiative (ONI: http://www.opennet.net), a partnership among groups at four leading global universities: Cambridge, Oxford, Harvard, and Toronto, funded by the John D. and Catherine T. MacArthur Foundation.

"Online censorship is growing in scale, scope, and sophistication around the world," said John Palfrey, Executive Director of the Berkman Center for Internet and Society and Clinical Professor of Law at Harvard Law School. "The regulation of the Internet has continued to grow over time – not surprising, given the importance of the medium. As Internet censorship and surveillance grow, there's reason to worry about the implications of these trends for human rights, political activism, and economic development around the world."

According to the study, censorship is expanding into new countries and becoming more sophisticated over time. Countries are not only blocking Web sites, such as pages online that show pornographic pictures, information about human rights, or YouTube but also applications, such as Skype and Google Maps.

The survey uncovers government activity in Asia, the Middle East and North Africa that denies citizens access to information--often about politics, sexuality, culture, or religion--that the governments deem too sensitive. Among the findings of ONI's survey are:

- 25 out of 41 countries surveyed showed evidence of filtering;
- Iran, China, and Saudi Arabia not only filter a wide range of topics, but also block a large amount of content related to those topics;
- South Korea's filtering efforts are very narrow in scope, but heavily censor one topic, North Korea;
- Countries engaged in substantial politically-motivated filtering include: Burma, China, Iran, Syria, Tunisia, and Vietnam;
- Saudi Arabia, Iran, Tunisia, and Yemen engage in substantial social content filtering;
- Burma, China, Iran, Pakistan and South Korea have the most encompassing national security filtering, targeting the websites related to border disputes, separatists, and extremists;
- No evidence of filtering was found in fourteen countries, including Afghanistan, Egypt, Iraq, Israel, West Bank and Gaza, Malaysia, Nepal, Venezuela and Zimbabwe, many of which one might expect to find Internet filtering.

-- more --

"These tests are the first comprehensive global assessment of Internet filtering practices," said Jonathan Zittrain, Professor of Internet Governance and Regulation at Oxford University. "Previously, Internet filtering generally has been described only by rumor and anecdote. We've confirmed that government-filtering is taking place in dozens of places around the world. It is becoming more pervasive and more subtle over time, often disguised as network errors. An essence of the rule of law is that citizens know when their governments are choosing to censor what they see, hear, and say. Otherwise they don't know what they don't know."

ONI conducted empirical testing for Internet blocking in forty-one countries in 2006. The 41 countries surveyed were chosen based on two criteria: where testing could be done safely (North Korea and Cuba were not included because of security concerns) and where there was the most to learn about government online surveillance. The research spanned thousands of websites across 120 different Internet Service Providers (ISPs), resulting in approximately 200,000 observations. ONI employs a multi-disciplinary approach that includes using a suite of sophisticated network interrogation tools and metrics and a global network of regionally based researchers and experts.

A number of countries in Europe and the United States and North America were not extensively tested this year because filtering practices of those countries are better understood. Direct comparisons between these Western countries to the countries examined in this survey is difficult because in Western countries, the private sector, rather than the government, often leads filtering efforts, and efforts are focused primarily to address copyright infringement issues, or to shield children from pornography. European practices are similar to those in North America, though less related to copyright and more filtering related to hate speech and racism.

A key finding of the study compares the breadth – the amount of information on a range of topics that is censored – and depth of filtering – the actual content that is blocked.

"States are applying ever more fine grained methods to limit and shape the information environment to which their citizens have access," said Ron Deibert, Director of the Citizen Lab at the Munk Centre for Internet Studies, University of Toronto. "Some states block access to a wide swathe of content across all of the categories in which we tested, while others tend to concentrate on one or two narrow baskets of content. South Korea, for example, tends to block access only to sites related to North Korea, many of which happen to be hosted in Japan."

The study finds three primary rationales for filtering: politics and power, leading to filtering of political opposition groups, common in many of the countries surveyed; social norms, leading to filtering of subjects deemed offensive to social norms, such as pornography, gay and lesbian content and gambling, also common in many of the countries surveyed; and security concerns, leading to the filtering of sites that could endanger national security, such as websites of separatist and radical groups, such as the Muslim Brotherhood in some countries in the Middle East.

"Cyberspace has become a strategic forum of competition between states, as well as between citizens and states," said Rafal Rohozinski, Research Fellow of the Cambridge Security Programme (Cambridge University). "Military and intelligence actors now consider the Internet to be an critical 'operational domain' that will be subject to shaping, controlled and regulation as much if not more than all previous media Our research suggests new and highly innovative trends in filtering and 'shaping' practices, including: 'event based filtering' where content was made inaccessible around elections and other

-- more --

politically sensitive moments; 'supply side' filtering where content producers denied access to their material to specific geographic locales; and, 'upstream filtering', where filtering occurs outside of national jurisdictions."

In future years, ONI will investigate Internet surveillance, and will develop methods to test for filtering of content available through "edge locations" (such as cybercafes), during elections (election monitoring), and from mobile networks, including SMS.

# # #

About the OpenNet Initiative

The OpenNet Initiative is a collaborative partnership between the Citizen Lab at the Munk Centre for International Studies at the University of Toronto, the Berkman Center for Internet & Society at Harvard Law School, the Advanced Network Research Group at the Cambridge Security Programme (University of Cambridge), and the Oxford Internet Institute at the University of Oxford. The OpenNet Initiative's work would not be possible without the generous support of its funders. The work of ONI has been supported by the Open Society Institute, the International Development Research Center (Canada), and the Ford Foundation at various stages since its inception. The John D. and Catherine T. MacArthur Foundation provided a $3 million grant that provided the core support for this first global survey.

For more information about the Open Net Initiative, please visit ONI's website: www.opennet.net.