What types of information are censored on the Internet? Who does this censoring? What tools exist to circumvent this censorship?

Introduction

Recent news of the failed “Cuban Twitter” and increased censorship in Turkey have reignited the attention paid to how the United States promotes its ideals abroad. Around the world, thousands of websites such as those focused on social media, political opposition, and human rights are blocked from public view, preventing the dissemination of great volumes of important information.

Though U.S. public diplomacy should not rely on the internet, it is increasingly becoming an important foreign policy tool. Recognizing this, the U.S. supports a variety of key tools allowing users to circumvent political censorship online.

This fact sheet provides a brief overview of the types of information blocking, a selection of countries of concern, several means to circumvent Internet censorship, and the U.S. role in censorship circumvention.

Key Takeaways:

• There are a variety of direct and indirect forms of online censorship.
• Foreign governments employ several of these techniques to enforce online censorship.
• Several types of tools are available for censorship circumvention.
• The U.S. is a major force in promoting anti-censorship tools.

Types of Censorship

There are four main categories of information blocking online:

1. Services, such as email or the web;
2. Content, such as that of political opposition websites, independent news sites, or human rights organizations;
3. Users, or blocking content by specific persons, such as human rights advocates or political dissidents;
4. Search engines, preventing search results from leading to specific websites.\(^1\)

In order to specify the content or category to be blocked, the blocker may use an IP address; port or protocol; domain name; URL; content signature, or keyword. These resources may be used to distinguish the exact content to be prevented from
appearing in a user’s search engine results or web browser.²

Furthermore, Internet censorship is carried out in several less-direct ways highlighted in recent news stories. These methods include, but are not limited to:

- **Restricting the speed** of the Internet to impede the viewing and downloading of information and materials;
- **Raising the cost** of Internet access to levels that are cost-prohibitive to the population;
- **Monitoring** activity to discourage the population from viewing specific websites or classes of websites because the population knows they are being watched.

**Known Blockers**

Around the world, several authoritarian regimes are especially known for their censorship of the web. China and Iran are two such countries.

- **China**
  - China uses a wide range of censorship techniques. The “Great Firewall” includes the blocking of Chinese microblog sites and other “politically sensitive sites” such as Facebook, Twitter, and The New York Times.³ ⁴ Reports that these sites were to be unblocked in Shanghai were later refuted by Chinese authorities.⁵
  - Facebook and Twitter have been blocked in mainland China since 2009.⁶ This censorship gave rise to Sina Weibo, a collection of microblogging sites similar to Twitter, which now boasts over 500 million users.⁷ ⁸ However, Weibo is still subject to censorship.⁹
  - Censorship is not always flawless. In January, a massive Internet outage affecting two-thirds of Chinese Internet traffic was allegedly caused by a malfunction of the “Great Firewall,” China’s Internet control infrastructure. For over an hour, millions of users were rerouted to servers owned, ironically, by a company that works to fight web censorship.¹⁰

- **Iran**
  - Iran censors web content in a variety of ways, including filtering websites, limiting Internet speed, and monitoring the web activity of individual citizens and bloggers.¹¹
  - In Iran, nearly half of the 500 most popular overall Internet sites are blocked. Many websites categorized as “art,” “news”, or “society” are blocked, as are websites focused on specific content such as politics or criticism of the government.¹² ¹³
  - Across the country, Internet speed is limited to a maximum of 128 kbps, about twice the speed of a dial-up connection but 50 times slower than a typical U.S. Internet connection.¹⁴ This speed, often as slow as 6 kbps, renders online information sharing extremely difficult and nearly impossible.¹⁵
  - Currently, Iran is collaborating with China to create a “National Information Network” in Iran,
essentially a “clean internet” that would provide access only to content that has been approved by the Iranian government.\textsuperscript{16, 17}

- **Turkey**
  - While Turkey is not as historically known for policing its networks, recent events have raised concerns.
  - A law was passed earlier this year allowing the country’s telecommunications authority to block websites without a court order.\textsuperscript{18}
  - In March, after an audio recording of a high-level meeting which reportedly implicated several high-level officials in a corruption investigation was leaked on Twitter, Prime Minister Recep Tayyip Erdogan called for the government to block the social media site.\textsuperscript{19}
  - Following this, YouTube was blocked after an audio recording of a high-level security meeting detailing possible action in Syria was uploaded to the site.\textsuperscript{20}
  - Turkish courts eventually reversed the blocking of both sites and Twitter. However, authorities defied the YouTube court order and continued to block the video sharing site.\textsuperscript{21, 22} Turkey finally unblocked YouTube access in early June, 2014.\textsuperscript{23}

- **Cuba**
  - Recent news has also highlighted Cuba’s censorship of the Internet, mainly done through excessive charges for access and slowing the speed of the Internet.\textsuperscript{24}
  - An initial lack of a telecommunications structure contributed to a very miniscule portion of the population having access to Internet at home; only a small percentage of Cubans have access to the Internet at work, which often consists of only the Cuban Intranet.\textsuperscript{25}
  - Government-run Internet cafes provide a common source of web access, but at an expense of $6-$10 per hour of unlimited use. In a country where the average weekly salary is only $20—access is cost-prohibitive for most.\textsuperscript{26}
  - Additionally, despite recent investments made in the country’s telecommunications structure, Cuba possesses the lowest connection speed in the Western Hemisphere, according to a Google Analytics study.\textsuperscript{27}

**Circumvention Tools**

There are four main types of technical tools used to circumvent Internet censorship.

- **Proxies**
  - The use of proxies in bypassing Internet censorship is useful for accessing specific blocked foreign websites. In this case, the user may utilize a foreign proxy server with compatible programs to access the website.\textsuperscript{28} A proxy server is essentially an “intermediary computer,” typically located
in another country, that is able to access the blocked site. This proxy is used to find and return information for the user while disguising his or her IP address.29

- **Tunneling/VPN**
  - A virtual private network, or VPN, allows a user to create an encrypted “tunnel” to a different computer which may then be used to access the Internet.30 The VPN/tunnel “wraps” the user’s web traffic to appear the same as other web traffic. As it is encrypted, the tunneled traffic is difficult to access or intercept by normal web filters.31

- **DNS-based filters**
  - The Domain Name System, or DNS, is a system that converts a website’s numeric IP address to a standard URL.32 DNS filters, while often put into place to block a specific web IP address, can also be used to bypass censorship by changing the DNS server of the provider of the website to be accessed. As long as the second server is not also blocked, it is possible to navigate around the censorship.33

- **Telescopic crypto (onion routing)**
  - Onion routing works by creating a system of network connections “that resist traffic analysis, eavesdropping, and other attacks” by outside parties.34 Essentially, it “distribut[es] [web activity] over several places on the Internet” so no one point can link to a user’s destination.35 The network then displays only that communication is occurring, not which parties are communicating with one another.36
  - Tor is one of the most well-known onion routing services, and was originally developed by the U.S. Navy to protect government communications. Today, it is used to create a wall of privacy between an internet user and another party monitoring the internet.37

**U.S. Role in Censorship Circumvention**

The United States plays a strong role in promoting censorship circumvention, funding programs and tools advancing Internet freedom, countering Internet censorship, supporting secure communications, and contributing to policy and research programs for those facing censorship, as well as other related objectives.38 Some examples and figures are highlighted below.

- From 2008 to 2012, the Department of State and USAID have contributed more than $100 million in support of Internet freedom programs.39 In 2013 alone, the U.S. Department of State and the U.S. Agency for International Development (USAID) gave $25 million in awards to groups focused on censorship circumvention.40

- The Broadcasting Board of Governors is an independent federal agency that oversees U.S. international broadcasting. Its target audience includes those in countries subject to internet and traditional media
censorship.\textsuperscript{41}

○ The Open Technology Fund, part of Radio Free Asia within the Board, funds numerous projects dedicated to advancing Internet freedom and circumventing its censorship. Projects include developing an iOS version of TextSecure, an encrypted text messaging application currently only available on Android devices; Cupcake Bridge, a browser extension that allows users to act as Tor bridges automatically, removing the need to install specialized software; and the translating of online toolkits from Security-in-a-box, a program designed to educate users on how to circumvent Internet censorship and remain undetected.\textsuperscript{42}

- The Tor Project receives significant funding from the U.S. Government.\textsuperscript{43}

- The U.S. is also a member of the Freedom Online Coalition, a collection of 22 like-minded countries working to advance “the ability of individuals to exercise their human rights and fundamental freedoms online.”\textsuperscript{44} The Coalition works with both civil society and the private sector, often working through multilateral organizations to protect and increase users’ rights on the Internet. A Coalition conference recently took place in Estonia in late April 2014.\textsuperscript{45}

Next Steps

Issues surrounding internet censorship have wide-reaching consequences not exclusively limited to freedom of information. The U.S. has a variety of interests it should consider as its role in promoting freedom of communication evolves. Some of these issues include:

- Cyber security as an issue of personal security—How do circumvention, security of electronic data, and protection of anonymity fit into this?
- How do anonymity tools threaten or increase security of the U.S.?
- What role should the U.S. play considering the increasing popularity of mobile platforms?
- How can the U.S. work with foreign parties, whether publics or governments, to increase freedom to access online information?
- What role do non-state actors play in anonymity, circumvention and censorship?
- How do U.S. laws affecting usage of the internet affect the global scene for online communication?

While censorship circumvention is vital to promoting U.S. foreign policy, it is also not always effective against countermeasures, and should not be the end goal. It is necessary for U.S. government leaders to work with their foreign counterparts to not only fund and develop censorship circumvention programs, but to foster a broader dialogue on the subject and call for increased awareness of the importance of an open Internet for the countries in which this is not a current reality.

Madeline Bersch is a Research Assistant & Intern at the American Security Project. She graduated from the University of Maryland College Park in May 2014 with a degree in Government & Politics and minors in Arabic and Global Terrorism.

Matthew Wallin is a Fellow at the American Security Project and holds a Master’s in Public Diplomacy from the University of Southern California.
2. Ibid.
6. Ibid.
9. Ibid.


34. Tor: Overview, Tor Project, https://www.torproject.org/about/overview.html.en#overview Accessed May 13, 2014


36. Tor: Overview, Tor Project, https://www.torproject.org/about/overview.html.en#overview Accessed May 13, 2014


The Honorable Gary Hart, Chairman
Senator Hart served the State of Colorado in the U.S. Senate and was a member of the Committee on Armed Services during his tenure.

Norman R. Augustine
Mr. Augustine was Chairman and Principal Officer of the American Red Cross for nine years and Chairman of the Council of the National Academy of Engineering.

The Hon. Donald Beyer
The Hon. Donald Beyer is the former United States Ambassador to Switzerland and Liechtenstein, as well as a former Lieutenant Governor and President of the Senate of Virginia.

Lieutenant General John Castellaw, USMC (Ret.)
John Castellaw is President of the Crockett Policy Institute (CPI), a non-partisan policy and research organization headquartered in Tennessee.

Brigadier General Stephen A. Cheney, USMC (Ret.)
Brigadier General Cheney is the Chief Executive Officer of ASP.

Lieutenant General Daniel Christman, USA (Ret.)
Lieutenant General Christman is Senior Vice President for International Affairs at the United States Chamber of Commerce.

Robert B. Crowe
Robert B. Crowe is a Partner of Nelson Mullins Riley & Scarborough in its Boston and Washington, DC offices. He is co-chair of the firm’s Government Relations practice.

Lee Cullum
Lee Cullum, at one time a commentator on the PBS NewsHour and “All Things Considered” on NPR, currently contributes to the Dallas Morning News and hosts “CEO.”

Nelson W. Cunningham
Nelson Cunningham is President of McLarty Associates.

Admiral William Fallon, USN (Ret.)
Admiral Fallon has led U.S. and Allied forces and played a leadership role in military and diplomatic matters at the highest levels of the U.S. government.

Raj Fernando
Raj Fernando is CEO and founder of Chopper Trading, a technology-based trading firm headquartered in Chicago.

Vice Admiral Lee Gunn, USN (Ret.)
Vice Admiral Gunn is the President of the Institute of Public Research at the CNA Corporation, a non-profit corporation in Virginia.

Lieutenant General Claudia Kennedy, USA (Ret.)
Lieutenant General Kennedy was the first woman to achieve the rank of three-star general in the United States Army.

General Lester L. Lyles, USAF (Ret.)
General Lyles retired from the United States Air Force after a distinguished 35 year career. He is presently Chairman of USAA, a member of the Defense Science Board, and a member of the President’s Intelligence Advisory Board.

Dennis Mehiel
Dennis Mehiel is the Principal Shareholder and Chairman of U.S. Corrugated, Inc.

Stuart Piltch
Stuart Piltch is the Co-Founder and Managing Director of Cambridge Advisory Group, an actuarial and benefits consulting firm based in Philadelphia.

Ed Reilly
Edward Reilly is CEO of Americas of FD International Limited, a leading global communications consultancy that is part of FTI Consulting, Inc.

Governor Christine Todd Whitman
Christine Todd Whitman is the President of the Whitman Strategy Group, a consulting firm that specializes in energy and environmental issues.
The American Security Project (ASP) is a nonpartisan organization created to educate the American public and the world about the changing nature of national security in the 21st Century.

Gone are the days when a nation’s security could be measured by bombers and battleships. Security in this new era requires harnessing all of America’s strengths: the force of our diplomacy; the might of our military; the vigor and competitiveness of our economy; and the power of our ideals.

We believe that America must lead in the pursuit of our common goals and shared security. We must confront international challenges with our partners and with all the tools at our disposal and address emerging problems before they become security crises. And to do this we must forge a bipartisan consensus here at home.

ASP brings together prominent American business leaders, former members of Congress, retired military flag officers, and prominent former government officials. ASP conducts research on a broad range of issues and engages and empowers the American public by taking its findings directly to them via events, traditional & new media, meetings, and publications.

We live in a time when the threats to our security are as complex and diverse as terrorism, nuclear proliferation, climate change, energy challenges, and our economic wellbeing. Partisan bickering and age old solutions simply won’t solve our problems. America – and the world - needs an honest dialogue about security that is as robust as it is realistic.

ASP exists to promote that dialogue, to forge that consensus, and to spur constructive action so that America meets the challenges to its security while seizing the opportunities that abound.

www.americansecurityproject.org