The Big List of Anti-Censorship/Anonymous Web Browsing Software

First off, why might you need to surf the web anonymously or through a proxy?

There are several reasons:

- You live in a country that censors the web. Moreover, you might get arrested if you try to access the wrong site.
- You live in the wrong country. Websites censor or block content based on where they think you live based on your IP address. A mundane example is content restricted to the US like full streaming episodes of TV shows.
- You don't want your web traffic to be tied to you. You don't websites keeping track of what you read or search for. As several online privacy debacles have shown, major sites and search engines are remarkably careless with their users' privacy.
- Your ISP decides to act as moral guardian and blocks access to sites it deems immoral.

For these reasons and more, I've compiled a list of free resources below that you can use to bypass or defeat censorship and protect your privacy.

The list will be continually updated.

Software

Email

SYMPA: Send anonymous email with this application

Web Browsing

Psiphon: Anonymous browsing based on networks of trust. Users need a username and password to logon to a unique web address before being allowed to use the proxy. Psiphon users don't need to install software, but users who want to run a psiphonode do.

Tor: This well-regarded application, recommended for use in conjunction with Firefox, routes your traffic through several other computers to increase your online safety and privacy.

UltraSurf 8: This application works with Internet Explorer to secure your browsing. A lock icon will appear on screen to indicated it is working. It is targeted mainly at Chinese net users, but English speakers should also check it out.

Sites (Web proxies)

Tip: Look for a CGI proxy if you need to logon to a site, you might also need to turn on Javascript

Browsing

Anonymouse: Browse the web through the web interface and even send anonymous emails.

BrowseAtWork: Features a Firefox extension for quick access

MySafeSurf: Features a provocative and suggestive banner

Proxify

Proxy.org: List thousands of working proxies

ProxyDom

Proxy 4 Free: Mixes transparent and anonymous proxies (if you need privacy, be sure to choose the ones labeled high anonymity)

Proxies sorted by Country (also from Proxy.org)

Super Privacy Guard: Great for users who want to tweak their proxy, supports URL encoding

VTunnel: supports URL encryption with RC4, which might fool some censorship filters

Email

TemporaryInbox: Get a disposable email, also support forwarding, Firefox extension available

Proxy Ranking Sites

CGIProxy.us

Global Proxies

HotProxies

Proxy Ring

Proxy Top List

Top Proxies

Top Proxy Sites

The Best Way to Leap China's Great Firewall

As Internet censorship surges around the world, researchers test circumvention tools at restricted cybercafes.
By David Talbot

As Internet filtering and censorship soars around the world, a comprehensive examination of leading circumvention technologies--carried out partly at Internet cafes in China, Vietnam, and South Korea--concludes that the leading tools work well but can slow Internet access significantly and, in some cases, present security holes.

"The issue of performance is a big one in terms of going to a higher proportion of users in countries where there is censorship," says John Palfrey, Harvard University Internet law professor and coauthor of the report released today by Harvard's Berkman Center for Internet and Society. "As with many Internet-based tools, the issue is one of scale," Palfrey adds. "Can you create an environment where it is easy enough and protective enough for people to use these tools? If not, they will remain a fringe activity."

In a related ongoing effort, the OpenNet Initiative--a project involving Harvard, the University of Toronto, Oxford University, and Cambridge University--is studying the spread of Internet censorship and surveillance worldwide. A forthcoming report will show a sharp rise in global filtering activity. Analyzing new data from 71 countries, OpenNet researchers have so far confirmed filtering in more than three dozen--up from 25 nations found to be filtering in a 2006 report, which looked at 46 nations in total. The new analysis, which will not be concluded for several more weeks, will also show greater blocking of social-networking sites such as Facebook and YouTube; increased filtering of blogging platforms, especially in the Middle East and North Africa; and an increase in examples of Western nations trying to block pornography, hate speech, and terrorism sites.

To get around Web restrictions, Internet users can install circumvention software. Such tools employ various approaches to route information around government or ISP blocks using proxy computers, or computers in nonfiltering nations that can fetch blocked pages and pass them on. Some versions allow people in filtered nations to tap their personal networks of friends and family abroad to acquire reliable and safe proxy-computer addresses. More complex systems bounce data around a few hops, with identifying data encrypted, to protect anonymity.

Ten tools--some commercial products and some open-source, nonprofit efforts--were tested for the new study, which was conducted partly in a lab setting at Harvard and partly in cybercafes in Beijing, Shanghai, Hanoi, and Seoul. Hal Roberts, a senior researcher at Berkman, visited the cafes and ran the circumvention tools through their paces. The best tools overall were found to be Ultrareach, Psiphon, and Tor, while Dynaweb and Anonymizer also scored well. Others suffered greater problems with usability or security.

"All of the tools we tested worked in the sense that if you sat in an Internet cafe in China and tried to bring up a site, you could do it," says Roberts. But a major problem, he says, was the long loading times of restricted pages, a function of limited bandwidth at proxies or the additional hops the data took to reach the cafe. "The only tool that was even marginally unpainful was Ultrareach," Roberts says, "but even for Ultrareach, it was anywhere from two to eight times slower than direct connection." In some cases, the extra time helps provide added security--notably for Tor.

The larger issue is that circumvention tools are only used by a few million people around the world--a small number, considering that China alone has some 300 million Internet users. The challenge ahead will include spreading the word more widely, increasing the availability of proxy computers, and enlisting more technical and financial support in the fight against censorship.

Circumvention research is supported by human-rights and civil-rights organizations, including Human Rights Watch and the Electronic Frontier Foundation, and by some Western governments. "It's easy to understand why governments and human rights funders would be interested in supporting censorship circumvention tools," notes the text of the report, which was coauthored by Palfrey, Roberts, and Ethan Zuckerman, who heads a blogging advocacy group called Global Voices. "As discourse shifts from traditional media to new participatory media, the ability to access and create online information becomes equivalent to the ability to read, listen, and speak freely."

谷歌

How China and Others Are Altering Web Traffic

"Invisible" servers let governments quietly intercept and modify their citizens' online communications.

"Invisible" servers let governments quietly intercept and modify their citizens' online communications.
By Robert Lemos

Google leveled new charges against China this week, claiming that the country has interfered with some citizens' access to the Internet giant's Gmail service, disguising the interference as technical glitches.
Security experts say that China is most likely using invisible intermediary servers, or "transparent proxies," to intercept and relay network messages while rapidly modifying the contents of those communications. This makes it possible to block e-mail messages while making it appear as if Gmail is malfunctioning.

- Companies regularly use transparent proxies to filter employees' Web access. Some ISPs have also used the technique to replace regular Web advertisements with those of their own. But it's becoming increasingly common for governments to use transparent proxies to censor and track dissidents and protestors. All traffic from a certain network is forced through the proxy, allowing communications to be monitored and modified on the fly. Intercepting and relaying traffic is known as a "man in the middle" attack.

- "What you are doing is rewriting the content as it is delivered back to the user," says Nicholas J. Percoco, the head of SpiderLabs, which is part of the security firm Trustwave. Percoco said China's ISP could track everyone who uses Gmail. To do this, it would "inject a JavaScript keystroke logger, which would record every keystroke they typed on the service."

- Defenses against the attack are few, especially if the Internet service provider has a valid cryptographic certificate, which all major national ISPs should have. Using a protocol known as HTTPS can prevent a man-in-the-middle attack, because it encrypts information in transit. However,, Microsoft revealed in a security advisory issued today that it had detected nine fraudulent certificates for popular Web sites, including Google Mail, Microsoft's Live service, and Yahoo's services. These fake certificates could also be used to intercept encrypted communications.

- The Chinese government is thought to have tightened communications in response to political unrest in the Middle East. Google discovered that problems with Gmail from within China came in the form of an attack that caused the Web application to freeze when a user took certain actions, such as clicking the "send" button.

- "There is no technical issue on our side—we have checked extensively," a Google spokesperson said in an e-mail statement. "This is a government blockage carefully designed to look like the problem is with Gmail."

- The attack appears to block the site only sporadically, halting access to the Web application for a few minutes and then allowing the user to again connect to Gmail, Google says.

- Other nations have used man-in-the-middle tactics to interfere with Web traffic. Tunisia took a similar approach to grabbing Facebook logins in order to perform surveillance on its citizens after widespread protests of the reign of Zine El Abidine Ben Ali. The protests followed massive unrest in other countries such as Yemen and Tunisia's next door neighbor, Libya.

- Facebook has become a major communications hub for protestors in many countries. The Tunisian government was "using the transparent proxy to hijack the sessions of the users' accounts and post positive things about the government to the people's Facebook accounts," says Percoco.

China's Internet Paradox

Will China's Web, like its larger economy, comfortably combine extraordinary growth with government repression?

China chat: A woman peruses the online discussion site QQ.com--one of China's most popular websites--in a Shanghai Internet café. Credit: Justin Guariglia

E-mail

On March 23, the day after Google pulled its search operations out of mainland China, a woman who uses the online pseudonym Xiaomi arose in her Shanghai apartment and sat down in her bedroom office for another day of outwitting Internet censorship. She leads a confederation of volunteer translators around the world who turn out Mandarin versions of Western journalism and scholarly works that are banned on China's Internet--and that wouldn't be available in Mandarin in any case. That day, working in a communal Google Docs account, she and her fellow volunteers completed translations of texts that ranged from a fresh *New York Times* interview with Google cofounder Sergey Brin to "The Limits of Authoritarian Resilience," a seven-year-old analysis of China's Communist Party from the *Journal of Democracy*.

What happened when Xiaomi hit "Post" reveals that the government's constraints have their limits. The pieces went live on a blog and a public Google Docs page. These links were broadcast to the nearly 4,000 people who follow her on Twitter (as @xiaomi2020), the 1,170 more who follow her on Google Buzz, and others on five Chinese Twitter clones. Although Blogspot and Twitter are blocked in China to those without circumvention software, anybody in the country can open the Google Docs page--at least for now. (The government did block Google Docs for a time last year but relented after protests from companies and universities.) Once posted, Xiaomi's translations are often reposted 10,000 times or more on blogs and bulletin-board-style discussion sites. There, they can survive for various lengths of time, though the hosting services--which are required to self-censor--generally take them down. The total readership may be orders of magnitude higher than the number of repostings, since each post is presumably read by many people, some of whom also copy the translations into group e-mails.

http://yyyyiiii.blogspot.com/

Bypass Censorship: Access Flickr in Iran, China, UAE, and Saudi Arabia

Not everyone loves Flickr. The photo sharing site has recently been banned in China (reported earlier). This move follows similar censorship by the governments of Iran, UAE, and Saudi Arabia.

However, it turns out that they aren't being too sophisticated about the ban on Flickr. If you have Firefox, you can install an extension called Access Flickr that lets you bypass the filter.

To be technical, the extension substitutes some parameters in the HTTP header that the government firewalls haven't been programmed to recognize and block. There isn't any need for proxies or more exotic measures like VPNs.

Research

My research and development activities are carried out primarily through the projects and collaborative partnershps of the Citizen Lab. The aim of the Citizen Lab is to monitor, analyze, and impact the exercise of power in cyberspace. The Citizen Lab accomplishes these goals through collaborative partnerships with leading edge research centers and organizations around the world, and through a pioneering “fusion” methodology that combines technical reconnaissance, field investigations, and data mining, analysis, and visualization. Below are some of the main collaborative research and development projects of which I am part:

infowar-monitor.net

The Information Warfare Monitor is a joint project of the Citizen Lab and The SecDev Group, (Ottawa Ontario). The aim of the Information Warfare Monitor is to monitor and analyze the exercise of power in cyberspace.

opennet.net

The OpenNet Initiative is a partnership with The Berkman Center for Internet & Society at Harvard Law School and The SecDev Group. The aim of the ONI is to document patterns of Internet censorship and surveillance world wide.

opennet.asia

The aim of **Opennet.Asia** is to engage academic, policy, and civil society stakeholders in each of the countries of the regions concerned by surveillance and censorship to build institutional capacity and networked resources to conduct research and public policy advocacy around those issues.

psi-LAB

PsiLab is a joint activity of the Citizen Lab and Psiphon Inc, oriented around advanced research of circumvention technologies, threat analysis, and the consideration of political and legal issues surrounding their use in denied environments.

ONI Releases Reports on Filtering in Asia, China

New research from the OpenNet Initiative reveals accelerating restrictions on Internet content as Asian governments shift to next generation controls. These new techniques go beyond blocking access to websites and are more informal and fluid, implemented at edges of the network, and are often backed up by increasingly restrictive and broadly interpreted laws.

The reports also point to an emerging inclination for states to actively engage in cyberspace as a way to achieve the same effects of information controls:

“Since 2006, many Asian governments have quickly realized the potential benefits of exploiting opportunities for conducting propaganda or public relations strategies over the Internet, even while cracking down on independent and critical voices thriving in these online spaces– an example of the evolution towards next generation controls,” said Ron Deibert, director of the Citizen Lab at the University of Toronto and one of four principal investigators at the ONI.

China continues to stand out amongst its neighbors due to its devotion of significant resources to consistently pursue both aggressive technical measures to pervasively filter information, as well as a regulatory regime aimed at perfecting these next-generation controls against private companies and other non-state actors.

These controls were evidenced recently in ONI’s analysis of China’s latest attempt at controlling the flow of information, Green Dam Youth Escort filtering software mandated for pre-installation on PCs sold in China starting July 1. “However, even China’s example demonstrates that restrictions on information are far from uniformly effective, and will meet resistance and be contested by the very groups they are intended to silence,” said Rafal Rohozinski, CEO of the SecDev Group and co-founder and principal investigator of ONI and ONI Asia.

“The Internet has been shown to be an especially effective tool for journalists, civil society activists and opposition leaders in Asia during elections or other national political crises,” said Al Alegre, regional coordinator for ONI Asia, which has developed into a regionally focused ONI network.

The reports for Asia, as well as Burma, China, Pakistan, and South Korea will be featured in a forthcoming MIT Press volume, Access Controlled: The Shaping of Rights, Rule, and Power in Cyberspace, to be published by MIT Press (2010). Access Controlled will include a series of analytical chapters and regional overviews that contribute to the developing discourse around global Internet regulation and censorship raised in the first ONI volume Access Denied: The Practice and Policy of Global Internet Filtering, (Cambridge: MIT Press) 2008.

The OpenNet Initiative is the global leader in the study of Internet censorship and a collaborative partnership of three leading academic institutions: the Citizen Lab at the Munk Centre for International Studies, University of Toronto; the SecDev Group (formerly the Advanced Network Research Group at the Cambridge Security Programme, Cambridge University); and the Berkman Center for Internet &

Society, Harvard University. The ONI’s principal investigators are Ronald J. Deibert
Director, The Citizen Lab, Munk Centre for International Studies, University of Toronto; Rafal Rohozinski, Former Director, Advanced Network Research Group, Cambridge Security Programme, University of Cambridge; and John Palfrey and Jonathan Zittrain of Harvard University.

ONI Asia is a collaborative research, advocacy, and networking project whose aim is to foster the respect for human rights online, and inform local, regional and global public policy. ONI Asia is funded by the International Development Research Council (IDRC), Canada.

View the reports on Asia and China here:

Asia Regional Overview
Internet Filtering in China