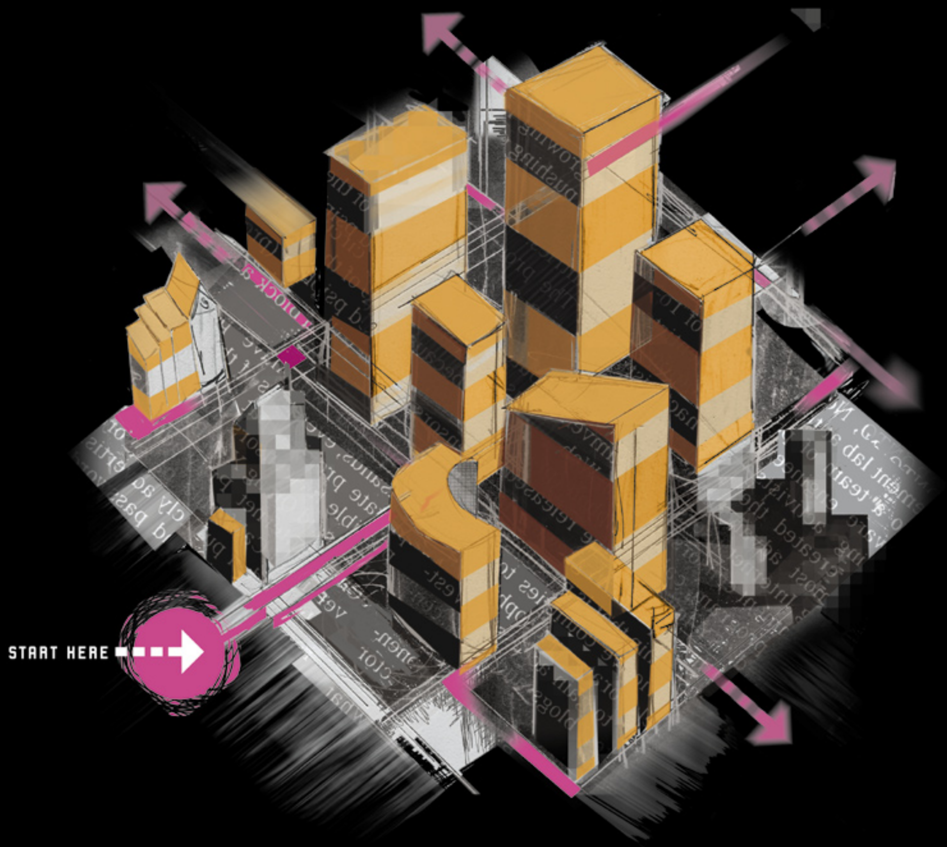


EVERYONE'S GUIDE TO BY-PASSING INTERNET CENSORSHIP

FOR CITIZENS WORLDWIDE

A CIVISEC PROJECT

The Citizen Lab
The University of Toronto
September, 2007

cover illustration by Jane Gowan

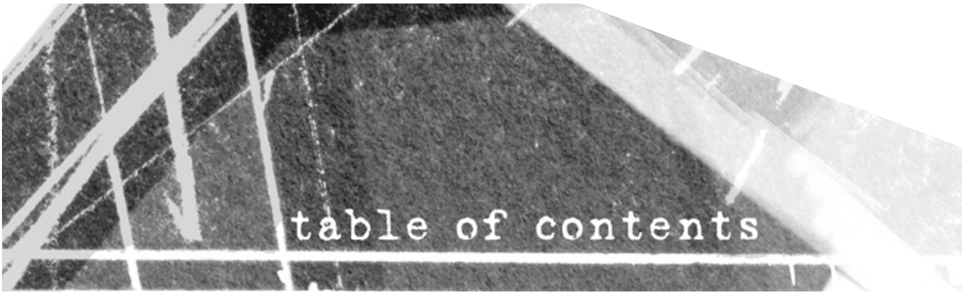


table of contents

Circumvention Technologies

Circumvention technologies are any tools, software, or methods used to bypass Internet filtering. These can range from complex computer programs to relatively simple manual steps, such as accessing a banned website stored on a search engine’s cache, instead of trying to access it directly.

Circumvention Providers

Circumvention providers install software on a computer in a non-filtered location and make connections to this computer available to those who access the Internet from a censored location. Circumvention providers can range from large commercial organizations offering circumvention services for a fee to individuals providing circumvention services for free.

Circumvention Users

Circumvention users are individuals who use circumvention technologies to bypass Internet content filtering.

introduction

Internet censorship, or content filtering, has become a major global problem.

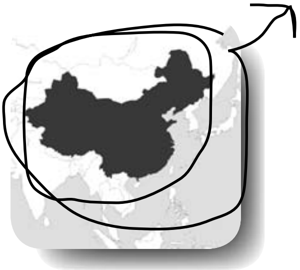
Whereas once it was assumed that states could not control Internet communications, according to research by the OpenNet Initiative (http.opennet.net) more than 25 countries now engage in Internet censorship practices. Those with the most pervasive filtering policies have been found to routinely block access to human rights organizations, news, blogs, and web services that challenge the status quo or are deemed threatening or undesirable. Others block access to single categories of Internet content, or intermittently to specific websites or network services to coincide with strategic events, such as elections or public demonstrations.

Although some states enact Internet filtering legislation, most do so with little or no transparency and public accountability. Most states do not reveal what information is being blocked, and rarely are there review or grievance mechanisms for affected citizens or content publishers. Compounding the problem is the increasing use of commercial filtering software, which is prone to over-blocking due to faulty categorization. Commercial filters block access to categorized lists of websites that are kept secret for proprietary reasons, even for customers. As a consequence, unaccountable private companies determine censorship rules in political environments where there is little public accountability or oversight. For example, commercial filtering software is used to censor the Internet in Burma, Tunisia, Yemen, Saudi Arabia, and Iran.

This guide is meant to introduce non-technical users to Internet censorship circumvention technologies, and help them choose which of them best suits their circumstances and needs.

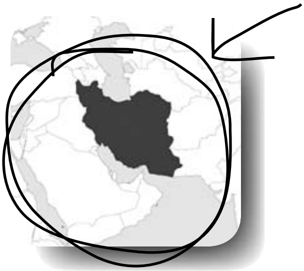
examples from the real world

Internet content filtering practices vary widely by country.



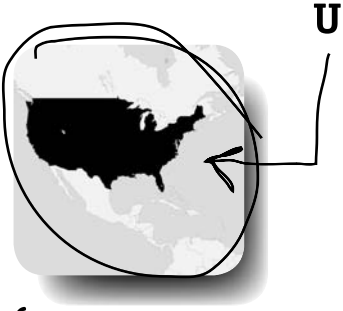
CHINA

In China, the government controls access to Internet content and online publishing by a combination of technical filtering methods and extensive regulations and guidelines. The technical filtering is implemented primarily at the national backbone level, with requests for information filtered for both banned Internet Protocol (IP) addresses and keywords. Although sometimes inconsistent, China's centralized system of content filtering ensures uniform blocking of access throughout the country to human rights, opposition political movements, Taiwanese and Tibetan independence, international news, and other websites. There is very little transparency about Internet filtering, and no public accountability process.



IRAN

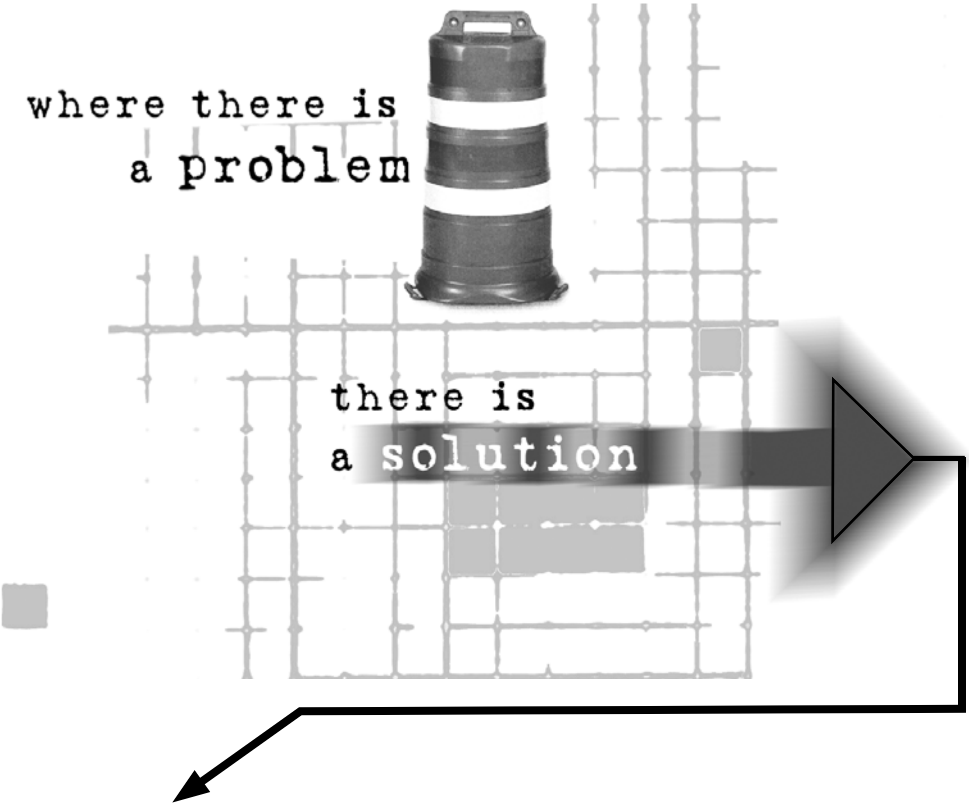
In Iran, there is no nationwide uniform filtering system. Instead, Internet Service Providers (ISPs) are responsible for implementing censorship following explicit guidelines stipulated by the state. Individual ISPs choose how they filter, with some using American commercial filtering software while others use more manual methods. Users accessing the Internet on different ISPs can experience significant variation of accessability to websites. Iran uses this system to filter Iran-related and Persian/Farsi language content critical of the regime, including politically sensitive sites, gay and lesbian content, women's rights sites, streaming media, and blogs. While there are debates wtihin government that openly acknowledge and discuss Internet content filtering policies, there is very little transparency about the specific content that is targeted for filtering.



U.S.A.

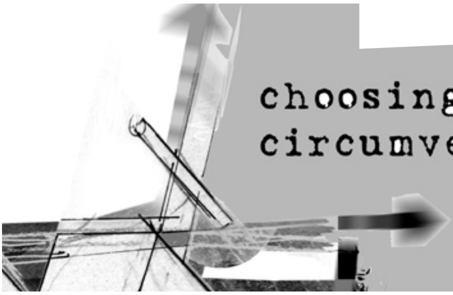
In the United States, public institutions (e.g., schools and libraries) are required by law (the Children's Internet Protection Act - CIPA) to use filtering software to block access to obscene, pornographic and other materials related to the sexual exploitation of children. Most implement the filtering policy by using commercial filtering technologies, which are prone to miscategorization and error. Researchers have found that commercial filtering technologies mistakenly block access to content related to women's health, gay and lesbian rights groups, and sexual education for teenagers.

In the face of this growing global problem, citizens around the world have sought solutions to evade government filters and exercise their basic human rights to access information of their own choosing.



The tools. methods, and strategies that are used to bypass Internet content filtering are referred to as ***circumvention technologies***.

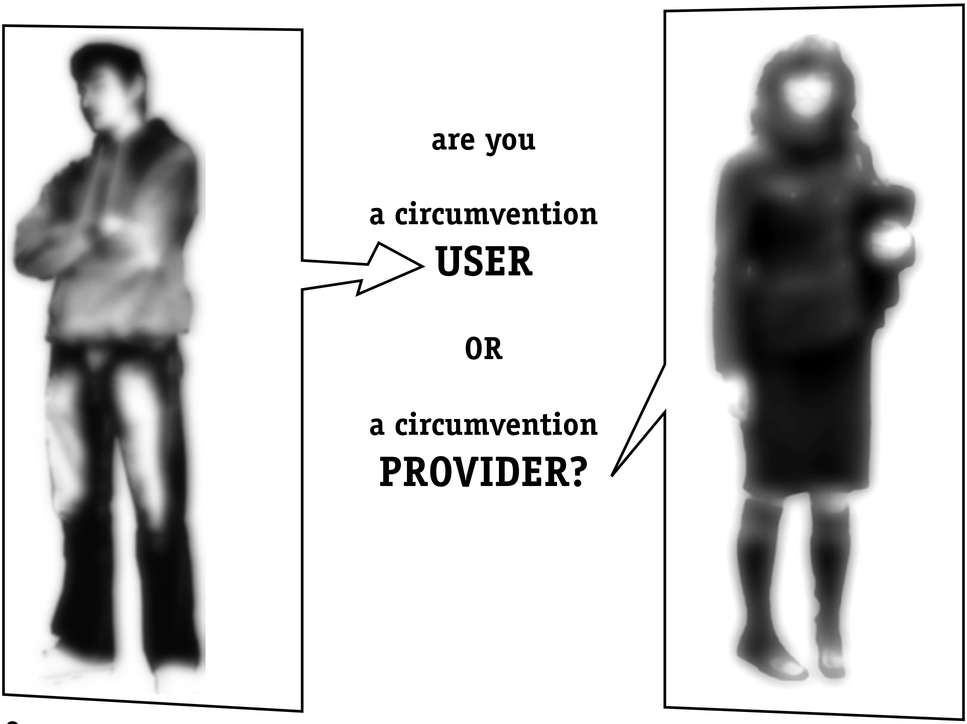
There are numerous circumvention technologies that can be used under a variety of different circumstances by a wide range of potential users. No one technology fits all of the different potential users and the circumstances within which they find themselves. Our view is that it is much better to think of circumvention technologies pragmatically as tools in a toolkit. Just as some tools are better for some jobs and not others, or require different levels of skill to employ responsibly, each circumvention technology should be approached in terms of how best it fits each user's unique problems, circumstances, and skillset.



choosing circumvention

Circumvention technologies often target different types of users with varying resources and levels of expertise. What may work well in one scenario may not be the best option in another.

When choosing a circumvention technology, it is important for the potential circumvention provider and user to determine what works best for their situation. The decision to use circumvention technology should be taken seriously, carefully analyzing the specific needs, available resources, and security concerns of everyone involved. There is a wide variety of technologies available for users who want to circumvent Internet filtering. However, using them for successful and stable circumvention service depends on a variety of factors, including the user's level of technical skill, potential security risk, and contacts available outside the censored jurisdiction. We outline some general considerations in choosing circumvention technologies for potential users and then for providers.



are you

a circumvention
USER

OR

a circumvention
PROVIDER?

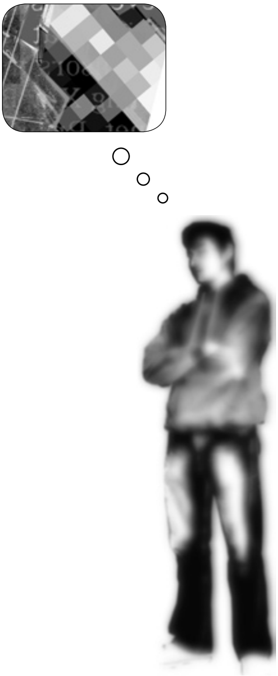
CONSIDERATIONS FOR THE CIRCUMVENTION USER: what, where, how

Do you want to access or publish information on the Internet?

Although closely related, accessing banned content, as opposed to publishing it, can involve different risks, strategies and technologies for the user. We have created a separate guide for those who want to circumvent Internet censorship to publish information online.

Are you accessing the Internet from a private or public computer?

Accessing the Internet from either your home or a public computer at an Internet cafe or public library involves a different set of considerations, and presents a range of possibilities for circumvention. For example, users who access the Internet from public computers or Internet cafés may not be able to install any software and will be restricted to web-based solutions. Others may want to use applications besides Web browsing (HTTP), such as e-mail (SMTP) and file transfers (FTP), and thus may want to install software on their computer workstation and to tweak their computer's settings. With your own private computer, you can install any software of your own choosing that you may not be able to install on a public Internet terminal. However doing so can impose additional risks, as there is now evidence on your computer of the use of circumvention technologies which, if seized by authorities, could lead to liabilities.



Public Internet access can offer anonymity that private computers cannot, although some require visitors to present personal identification and/or monitor visitors' usage. Whether you circumvent censorship through your home or a public terminal, it is always important to understand as fully as possible the terms and conditions of the service that is being provided.

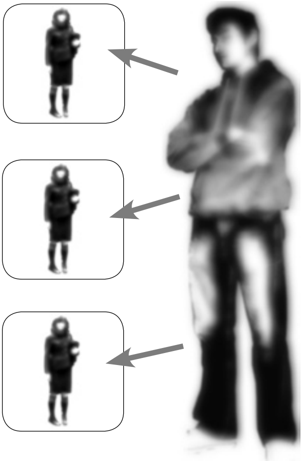
choosing circumvention cont'd

CONSIDERATIONS FOR THE CIRCUMVENTION USER: **who** do you know?

Do you have any connections to or availability of trusted out-of-country contacts (e.g., friends, family members, colleagues)?

Since circumventing Internet censorship involves making connections to a computer outside of the jurisdiction in which the censorship takes place, an important factor for consideration is whether you know and trust someone or group outside of the country who is willing to provide circumvention services for you. Many users who circumvent censorship do so by connecting to open public proxy computers whose connection information is advertised in some manner. Users should be aware that these are the least secure by definition, since a user can never be certain that an adversary has not set up a trap, or "honey pot", to entice dissidents.

Having someone you know and trust set up a connection instead is a better option, but it is not without its own set of risks and considerations. Providers can monitor every thing you do online, including all of the sites you visit. That is why it is essential that you fully trust the person or organization that is providing the circumvention service for you. Successful, long-term and stable circumvention is greatly enhanced by having a trusted contact in a non-filtered location.



Are you willing to pay and put your trust into a third party organization to access or publish information on the Internet?

If you do not have access to trusted friends and family members outside of your jurisdiction then you may have to put your trust into a third party. There are many commercial providers that offer circumvention services for a fee. If you are able to afford this option, be careful to explore the terms and conditions of the service and the privacy policy. Commercial services may offer anonymity to surf the Internet, but not anonymity from the commercial provider itself. If compelled by law, the commercial service may turn over all of their records, and your personal information.

choosing circumvention cont'd

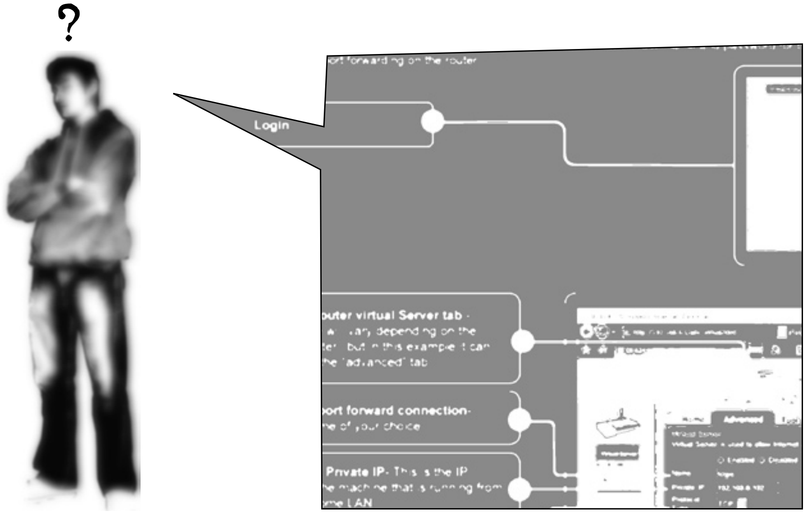
CONSIDERATIONS FOR THE CIRCUMVENTION USER: **what** do you know?

What is your level of technical expertise? Do you consider yourself a beginner, intermediate, or expert computer user?

The greater your level of technical expertise the more your circumvention options increase. Some users may find the installation, set-up process, and use of circumvention technologies to be too onerous or beyond their level of expertise. Although it is always possible to invest time and learn how to use even the most seemingly complex software, be careful: the incorrect installation and use of circumvention technologies may put you at considerable risk.

What language of use is acceptable/preferable to you? Do you require technologies that operate other than English?

Most circumvention technologies are designed with user interfaces and instructions in English, although many also offer versions of their systems and user guides in other languages. If you are consulting a translated user's manual, be sure that the translations you use match the version of the software you are employing as the two may not necessarily match.


?
ort forwarding on the router
Login
outer virtual Server tab -
w vary depending on the
ter but in this example it can
the 'advanced' tab
port forward connection-
me of your choice
Private IP- This is the IP
he machine that is running from
ome LAN
Advanced

choosing circumvention

cont'd

CONSIDERATIONS FOR THE CIRCUMVENTION USER: safety & security

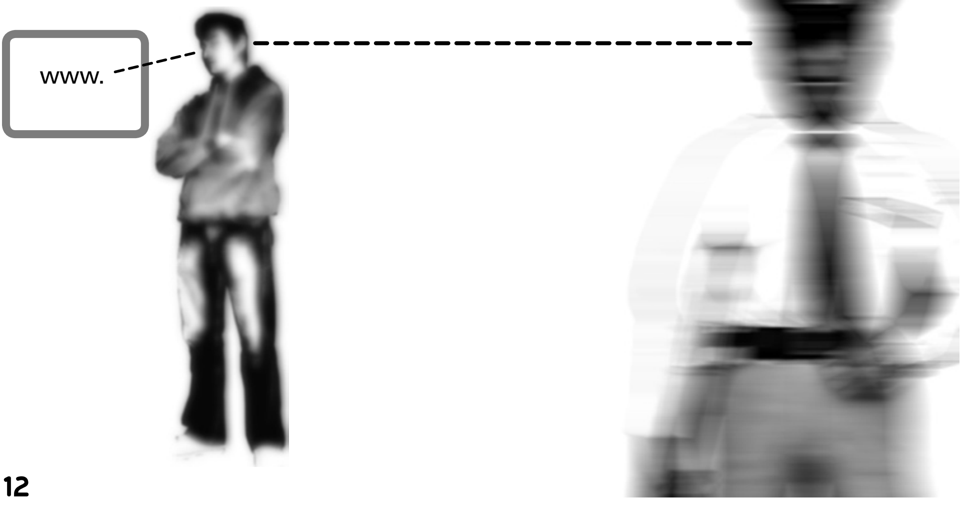
Are you accessing content that is highly critical of and is considered a security threat to the country in which you live?

Is there a precedent for arrests for the practice of circumventing Internet censorship in your country?

Do you have any affiliations with high profile groups that are known to be on your government's watch list?

Accessing banned content can be a serious violation of the law, especially if the information you are visiting is considered a national security threat. If you are consistently accessing this type of content, you should choose circumvention technologies that offer the greatest anonymity and security. However, there is usually a trade-off between ease-of-use and security so be prepared to spend extra time and effort in order to minimize risks.

If you are associated with a high profile rights organization or dissident group, then you may be on your government's watch list and you should take extra precautions in carefully choosing your circumvention technologies. You may want to assume that you are being monitored and that your computer could be seized at any time. Avoid circumvention technologies that require installation on your computer. If possible, access the Internet from a range of different anonymous public terminals instead.



choosing circumvention cont'd

CONSIDERATIONS FOR THE CIRCUMVENTION USER: identity

Is protecting your identity online of paramount importance to you? Do you want to surf and/or publish anonymously?

Circumvention and anonymity are different. Anonymous systems protect your identity from the website you are connecting to and from the anonymity system itself. They can be used for circumvention, but are not designed for this purpose and thus can easily be blocked. Circumvention systems are designed to get around blocking but do not protect your identity from the circumvention provider.

Do not mistake open public proxies for anonymous systems - they are not. Although they may not ask for personal information, they can view and record the location of the computer from which you are connecting and all of the websites you visit through them.

Commercial services which advertize anonymous surfing may still record your connection information and the websites you visit. Make sure you fully understand the terms and conditions of their use.

There are a number of strategies that you can follow if you want to publish online anonymously. The Citizen Lab has created a separate guide on circumvention for publishing online that includes a section on anonymous publishing.

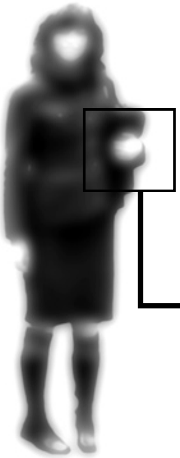
choosing circumvention
cont'd

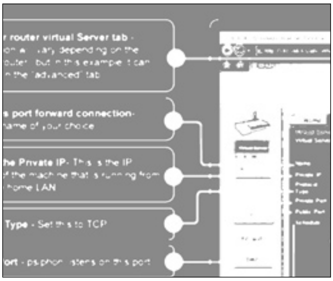
CONSIDERATIONS FOR THE CIRCUMVENTION PROVIDER: safety first

Setting up a circumvention technology for someone is a great way to give a helping hand to others to exercise their basic human rights of access to information and freedom of speech. However, it is a choice that carries with it a heavy responsiblity and several considerations. Above all else, the safety of your users must be your primary concern.

What is your level of technical expertise? Do you consider yourself a beginner, intermediate, or expert computer user?

Setting up and hosting a circumvention technology server can be a time-consuming and complex task depending on the circumvention system. Some require the download and installation of several different pieces of software. Almost all of them will entail some configuration to accommodate your own particular network environment. If you are running your Internet connection through a home router or firewall, for example, there may be some customization of your circumvention system. Some circumvention technologies have very clear and helpful documentation and user guides while others do not. **Be sure that you choose a technology that matches your skill level and abilities,** as setting up a system improperly could jeopardize the security of your user(s). **Make sure that you are also comfortable maintaing your system**, as an outdated or constantly interrupted technology can frustrate and needlessly endanger users in censored locations.




r router virtual Server tab - on w vary depending on the outer but in this example it can n the "advanced" tab
s port forward connection- name of your choice
he Private IP- This is the IP f the machine that is running from home LAN
Type - Set this to TCP
ort - psiphon listens on this port

choosing circumvention
cont'd

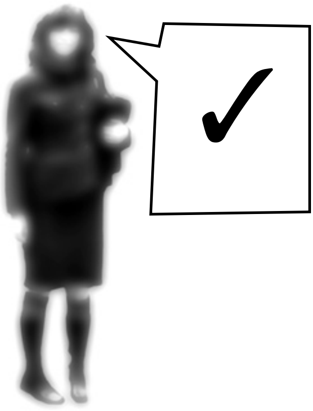
CONSIDERATIONS FOR THE CIRCUMVENTION PROVIDER: your users

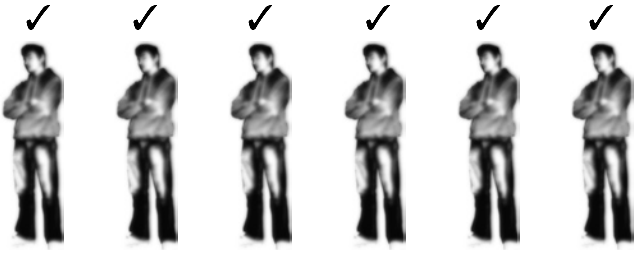
What is the number of users you expect or want to accommodate and what is your available bandwidth?

The number of users you allow to surf through your computer will affect your computer's processing capabilities and your connection speeds, affecting not only what you do but what circumvention users can do. The more users you have, the more complicated it will be to monitor their usage (if necessary) and manage their accounts. **Make sure that you offer circumvention services only to the number of users you and your computer can comfortably handle.**

What will you allow your users to do through your connection? Would you want to know what information they are accessing or publishing? What are you going to do with their surfing records?

Setting up a circumvention service means that you will be able to monitor all of the usage that runs through it. Having this capability means that you can decide what information you will allow users to retrieve or publish. Some circumvention systems make this feature easier to employ than others, but even those that do not still leave traces on your computer of the user's activity. You must decide for yourself what information you will choose to view, archive, and/or discard. If you choose to discard this information, make sure that you do it properly as even deleted information can leave traces. Above all, make sure that you let your users know what your standard operating procedure will be concerning the information they leave on your computer and what they can do through your circumvention system. **Communicate a clear policy to your users.**





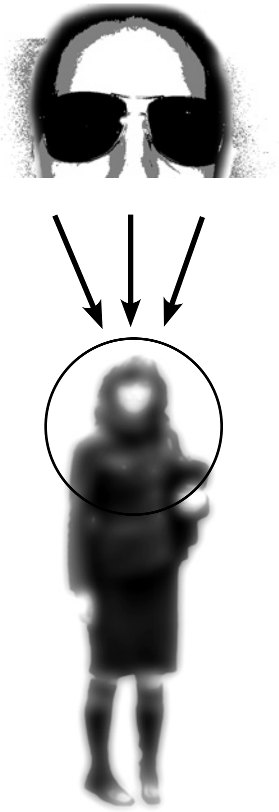
choosing circumvention

cont'd

CONSIDERATIONS FOR THE CIRCUMVENTION PROVIDER: risks

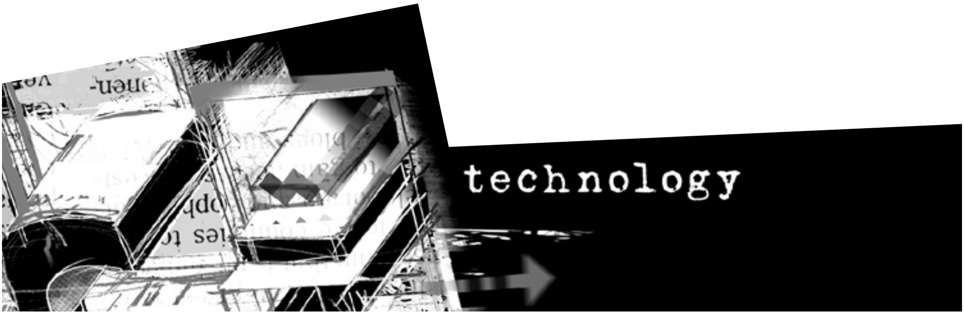
What are your potential security and legal risks of hosting circumvention technologies? Does your ISP or government restrict this type of service?

The risks of hosting circumvention technologies are not as great as they are for users of circumvention technologies, but they are not zero. You are almost certainly responsible for everything that is done through your computer using your Internet connection. If someone visits websites or posts information through your circumvention service that is illegal you may be held liable. A less likely but nonetheless signifcant risk concerns the possibilty of you becoming a target of foreign agents of the country in which your service is offered. Make sure that you understand the potential security and legal risks of hosting circumvention technologies from the perspective of both your ISP and your own government.



examples from the real world

At 11:15 am on February 8, 2006, unkown assailants forcibly entered Peter Yuan Li's Atlanta, GA (USA) home, bound and beat him, and then left with several laptops and other files belonging to him. An information technology specialist from Princeton University and a Falun Gong practitioner, Peter Yuan Li had been maintaining several forums in the United States where users within China could tunnel through China's national firewalls to read and post information on the banned religious movement. Although there is no conclusive evidence to prove the case, Mr. Li believes that the assailants were operatives of the Chinese government trying to shut down his service.



WEB-BASED CIRCUMVENTION SYSTEMS

Web-based circumvention systems are special web pages that allow users to submit a URL and have the web-based circumventor retrieve the requested web page. There is no connection between the user and the requested website as the circumventor transparently proxies the request allowing the user to browse blocked websites seamlessly. Since the web addresses of public circumventors are widely known, most Internet filtering applications already have these services on their block lists, as do many countries that filter at the national level. Web-based circumvention systems could be a good choice for the users connecting with no trusted out of country contacts, assuming the pages are not yet blocked.

NOTE: Although some may advertise themselves as "anonymous" many web-based circumvention are not. Some may not even be encrypted. It is important to remember that encrypted websites begin with "https" and are signified by the open lock icon in your web browser moving to the locked position. If you send your web requests unencrypted, they can be easily intercepted any step along the way of transmission, from your home or office router to your ISP.

WEB-BASED CIRCUMVENTION SYSTEMS: the list

Proxify
https://proxify.com/

StupidCensorship
https://stupidcensorship.com/

Proxify and Stupid Censorship are encrypted, public, web-based circumvention systems. A user in a censored country simply visits one of the web sites and then inputs their destination. Since these web services are public, however, they are blocked in many countries and by most filtering applications.

WEB-BASED CIRCUMVENTION SYSTEMS: the list cont’d

CGIProxy

http://www.jmarshall.com/

CGIProxy is the engine that most web-based circumvention systems use.

Private web-based circumvention systems turn a computer into a personal, encrypted server capable of retrieving and displaying web pages to users of the server connecting remotely. Private web-based circumventors include providers, who install and run circumvention software in an uncensored jurisdiction, and users, who access the service from a jurisdiction that censors the Internet. The circumvention provider grows his/her private network based on social relations of trust and private communications making it difficult for censors to find and block.

psiphon

http://psiphon.civisec.org/

psiphon turns a regular home computer into a personal, encrypted server capable of retrieving and displaying web pages anywhere. The user in the uncensored country downloads the software and installs it on his/her home computer. psiphon is free and open source, and comes in Linux and Windows versions. It is easy to install, and comes with a very detailed and easy-to-follow user guide. If your computer is behind a home router it may require some configuration. Once installed, the psiphon provider sends the connection information to users in censored jurisdictions by the most secure means available. The censored user does not have to install any software but simply types a URL into the psiphon “blue bar.” This means that the psiphon circumvention system can be accessed from anywhere. Since the locations of psiphon-enabled computers are private, they are difficult for censors to find and block.

Peacefire/Circumventor

http://peacefire.org/

Peacefire/Circumventor is a circumvention system nearly identical in principle and method to psiphon. However, It can be difficult to install. Three different software packages must be downloaded and installed, and and if your computer is behind a home router it may require additional configuration. Although Peacefire/Circumventor provides some setup help, there is not a detailed user guide as there is with psiphon. Otherwise, Peacefire/Circumventor works along the same principles as psiphon.

TUNNELING SOFTWARE

Tunneling encapsulates one form of traffic inside of other forms of traffic. Typically, insecure, unencrypted traffic is tuhnneled within an encrypted connection. The normal services on the user's computer are available, but run through the tunnel to the non-filtered computer which forwards the user's requests and their responses transparently. Users with contacts in a non-filtered country can set up private tunneling services while those without contacts can purchase commercial tunneling services. "Web" tunneling software restricts the tunneling to web traffic so that web browsers will function but not other applications. "Application" tunneling software allows one to tunnel multiple Internet applications, such as email clients and instant messengers.

WEB TUNNELING SOFTWARE: Free

UltraReach

http://www.ultrareach.com/

Ulreareach has created anti-censoprship software known as UltraSurf. UltraReach provides a client download for Windows that the user in the censored country downloads (installation is not required) on his or her own computer. It is free software and is available in English and Chinese. Once started, the application opens an Internet Explorer application that is automaticaly configured to allow the user to browse websites through UltraSurf. Other browsers must be manually configured. By default, the connection is encrypted and various techniques are used to find an unblocked IP address.

UltraSurf is an excellent choice for non-technical users who are willing to trust a third-party and require free web browsing at reasonable speeds.

Since the UltraReach website is often already blocked in some countries, a user in a censored jurisdiction may have to acquire the software through a third party. Even though the website may be blocked, the service could still be accessible as measures are taken to acquire unblocked IP addresses in a variety of ways. However, even these could be blocked by a very determined censor.

WEB TUNNELING SOFTWARE: Free

FreeGate

http://www.dit-inc.us

Freegate is an anti-censorship technology developed by DynaWeb, similar in many ways to UltraSurf. Unlike UltraSurf, however, Freegate does not encrypt the URL by default. If users want to encrypt the URL request, they have to download another software package and specially configure Freegate.

FreeGate is a good choice for expert users who are more concerned with circumvention than security, are willing to trust a third party, do some manual configuration, and require free web browsing at reasonable speeds.

As with UltraSurf, the Freegate website is blocked in many censored jursidications, and so users must acquire the software through a third party. Likewise, the service itself may be blocked, although users can manually insert unblocked IP addresses into Freegate.

WEB TUNNELING SOFTWARE: Pay

Anonymizer

http://anonymizer.com

Anonymizer provides a client download for Windows that a user in a censored country installs on their computer. After completing the easy installation process, the user enables the "Anonymous Surfing (tm)" option after which their traffic is transparently tunneled through Anonymizer. However, to ensure security the user must enable the "Surfing Security (tm) SSL Encryption" so that all traffic is encrypted with HTTPS/SSL. This option is disabled by default. The software also provides other services, such as "Digital Shredder", Anti-Spyware, and disposable email addresses.

Anonymizer is an excellent choice for users that are not technically proficient and are willing to pay and trust a third party for encrypted web browsing at high speeds. Since the Anonymizer website is often blocked in many jurisdictions, a user may have to acquire the software through a third party. While the service may still be accessiible in spite of the filtering of the website, the service itself could be easily blocked by a determined censor. Since the application must be installed, it may not be suitable for public terminals or high-risk users whose computers are at risk of being seized.

WEB TUNNELING SOFTWARE: Pay

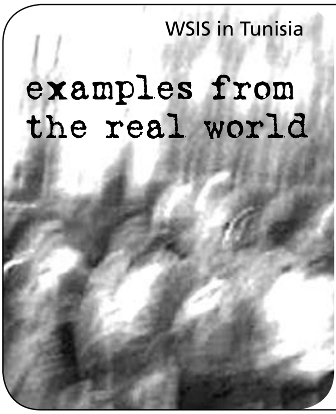
Ghost Surf

http://tenebril.com

GhostSurf provides a client download for Windows that a user in a censored country installs on their computer. After completing the installation, the software configures the Internet Explorer browser automaticaly. All other browsers must be manually configured. The software is set to "Normal" by default, meaning all traffic is in plaintext and easily intercepted. To encrypt the traffic, the user must change this setting to "Secure," the highest setting (the "Anonymous" setting is misleading, only blocking cookies, not making traffic anonymous). Once the software is configured with the "Secure" setting, and the user has modified the browser settings if not using Internet Explorer, the user's traffic is encrypted and is routed through Ghost Surf servers.

Ghost Surf is a good choice for those who are somewhat technically proficient and are willing to pay and trust a third party for a fast connection.

As with Anonymzer, since the Ghost Surf website is often blocked in many jurisdictions, a user may have to acquire the software through a third party. While the service may still be accessible in spite of the filtering of the website, the service itself could be easily blocked by a determined censor. Since the application must be installed, it may not be suitable for public terminals or high-risk users whose computers are at risk of being seized.



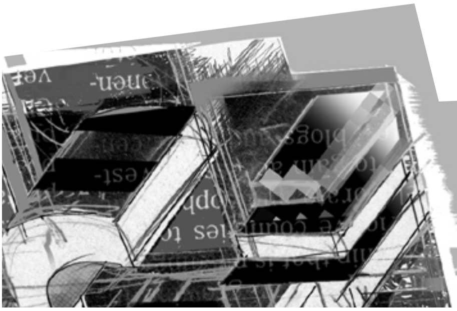
WSIS in Tunisia

examples from the real world

The World Summit on Information Society II (WSIS) was held in Tunis, Tunisia in 2006. Tunisia filters access to content extensively, including websites critical of the government's human rights record.

WSIS was held in a building that had two sections, each with different Internet access protocols. In the official proceedings' section, Internet access was unfettered. In a separate section reserved for NGOs and journalists, Internet access was managed through a Tunisian ISP, which filtered content heavily using the American commercial product, Smartfilter.

An NGO with a booth located on the filtered side set up a proxy with an SSH-D tunnel to their home office computer, based in the Netherlands. The NGO then informed members of the port number of the browser, allowing them to bypass Tunisian filtering.



APPLICATION TUNNELING SOFTWARE: Free

GPass

http://gpass1.com/

GPass provides a client download for Windows that a user in a censored jurisdiction downloads (there is an optional installer) on their computer. It is free software and is available in English and Chinese. Once GPass is started, the icons of applications to be proxied through Gpass can be dragged and dropped into the Gpass interface. When these application are started via Gpass, they are automatically confiugured to run through the service. By default, Internet Explorer, Windows Media Player, and the default email client are already configured. By default, the connection is encrypted and various techniques are used to find and connect to an unblocked IP address. The application provides reasonable speeds and has the ability to store encrypted bookmarks and other files.

GPass is an excellent choice for non-technical users who are willing to trust a third party and require encrypted, free tunneling for services other than browsing (http) at reasonable speeds.

As with Anonymzer and others, since the Gpass website is often already blocked in many jurisdictions and by filtering applications, a user may have to acquire the software through a third party. To counteract the possible filtering of the service, measures are taken to automatically find unblocked IP addresses. Since the application must be installed, it may not be suitable for public terminals or high-risk users whose computers are at risk of being seized.

APPLICATION TUNNELING SOFTWARE: Free

HTTP Tunnel

http://www.http-tunnel.com/

HTTP Tunnel is another client download for Windows that a user in the censored country downloads and installs on their computer. Much like psiphon and Peacefire/ Circumventor, HTTP Tunnel also provides a “server” that a user in an uncensored country can download to setup a private service for someone in a censored country. The HTTP Tunnel can be used for free although a pay service is also available. Users must manually configure applications, such as web browsers, email clients, and instant messengers to use HTTP Tunnel.

HTTP Tunnel is a good choice for technical users who are more concerned with circumvention than security and are willing to trust a third party, do some manual configuration and require tunneling for services other than browsing (http) at reasonable speeds. HTTP tunnel traffic does not appear to be not encrypted, just encoded. The latter is simply a different way of expressing information, not a way to keep information secret, as the former.

As with many others, since the HTTP Tunnel website is often already blocked in many jurisdictions and by filtering applications, a user may have to acquire the software through a third party. A determined censor could also block the service of HTTP Tunnel, although measures could be taken to counter-act such censoring by a technically proficient user. Since the application must be installed, it may not be suitable for public terminals or high-risk users whose computers are at risk of being seized.

APPLICATION TUNNELING SOFTWARE: Pay

Relakks

https://www.relakks.com/

Relakks provides a pay-service called Relakks Safe Surf. It is a Virtual Private Network (VPN) system that uses an encrypted tunnel to transport traffic from the user in the censored country through the Relakks servers. It uses the native VPN clients on the Windows and Mac platforms, so users are not required to install any software. Many different applications can be tunneled over the VPN, such as email, web browsing, and instant messenging.

Relakks Safe Surf is an good choice for those users who are not technically proficient and are willing to pay and trust a third party for a encrypted VPN. However, Relakks could be easily blocked.

Guardster/SSH

http://www.guardster.com/

In addition to a free, non-encrypted, web-based circumvention system, Guardster provides both an encrypted web-based circumvention system and a Secure Shell (SSH) Tunnel for a fee. A variety of software applications, including web browsers and email clients, can be tunneled through the encrypted SSH tunnel of Guardster.

Guardster/SSH is an good choice for those users who are not technically proficient and are willing to pay and trust a third party for a encrypted tunnel.

As with many others, since the Guardster/SSH website is often already blocked in many jurisdictions and by filtering applications, a user may have to acquire the software through a third party. A determined censor could also block the service of Guardster/SSH.

ANONYMOUS COMMUNICATIONS SYSTEMS

Anonymous technologies conceal a user’s IP address from the server hosting the web site visited by the user. Some, but not all, anonymous technologies conceal the user’s IP address from the anonymizing service itself and encrypt the traffic between the user and the service. Since users of anonymous technologies make requests for web content through a proxy service, instead of to the server hosting the content directly, anonymous technologies can be a useful way to bypass Internet censorship. However, some anonymous technologies require users to download software and can be easily bllocked by authorities.

JAP ANON

http://anon.inf.tu-dresden.de/index_en.html

JAP ANON provides a client download for Windows/Mac/Linux that the user in a censored country downloads and installs on their computer. It is available in English and several European languages. The user must select a “mix” through which to route traffic and then follow the instructions provided to configure the web browser to use JAP ANON. The “mix” is a set of internediaries through which a request is routed and since many requests are moving through the mix neither the operators of the mix nor the host being requested through the mix know the user’s true identity. However, there are varying levels of anonymity as some use a “single mix” while others use “mix cascades.” There is also a pay serverice for access to higher speeds and more anoymous mixes.

JAP ANON is a good choice for technical users who require anonymity along with circumvention service for web browsing at reasonable speeds.

Since the JAP ANON website is often already blocked in many countries a user in a censored country may have to acquire the software through a third party. The service may still be accessiible if the website is blocked, although a determined censor could also block the service . Since the application must be installed it may not be suitable for public terminals or high risk users whose equipment may be seized.

ANONYMOUS COMMUNICATIONS SYSTEMS

Tor

http://tor.eff.org

Tor is a free, anonymous communications system that works by routing web requests through a series of routers each of which peels away a layer of encryption so that no individual router on the network can identify the source or the destination of the request. It is an excellent choice for those who require strong anonymity because it would be extremely difficult for a government to monitor your communications through the Tor network. Tor also allows users to tunnel a variety of other protocols through its network, such as instant messaging traffic and email. It also has a feature known as “hidden services” that allows users to anonymously publish their own web pages that are only accessible via Tor.

It presently requires a client dowload, so is likely not appropriate for public terminals and implies a significant risk for those whose computers may be seized. It is available in multiple languages and is open source, and has a very dedicated, thriving development network and documentation. After installation, the Tor service begins and the user may use the preferred Firefox broswer, which comes with “Torbutton” so Tor can be easily toggled on and off. Other browsers require manual configuration.

Tor is an excellent choice for technical users who require strong anonymity along with circumvention service for multiple applications at slow speeds.

Even though the Tor website is blocked in some countries, the service is not. However, a determined govenrment could easily block Tor if they choose to do so. However, developers are working on blocking resistance solutions. Because of the multiple routers through which Tor traffic passes, surfing the Internet via Tor can be slow. Tor requires considerable computer skils; and is not for the novice.

ANONYMOUS COMMUNICATIONS SYSTEMS

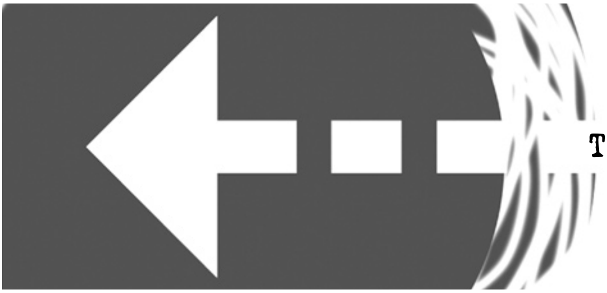
I2P

http://www.i2p.net

I2P is an anonymization network that is primarily intended for users to publish content aonoymously and access content anonymously through I2P. However, it can also be used to surf the Internet anonymously. I2P provides a client download for Windows/ Mac/Linux that a user in a censored country downloads and installs on their computer. The user's browser must be manually configured to point through the I2P network.

I2P is a good choice for technical users who require anonymity, primaily for publishing but also for circumventing filters at slow speeds.

Since the I2P website is often already blocked in many countries a user in a censored country may have to acquire the software through a third party. The service may still be accessible although it too could be blocked by a determined censor. Since the application must be installed it may not be suitable for public terminals or for high risk users whose computers may be seized.



Tricks of the Trade

"Cached" Pages

Many search engine provide copies of web pages, known as cached pages, of the original pages they index. When searching for a website, look for a small link labelled "cached" next to your search results. Since you are retrieving a copy of the blocked page from the search engine's servers, and not form the blocked website itself, you may be able to access the censored content. However, some countries have targetted caching services for blocking.

Example: Google Cache

Translation Services

There are many translation services available on the Internet, often provided by search engines. If you access a website through the translation service, it is the translation service that is accessing the blocked site. This allows you to read the censored content without directly connecting to the blocked website.

Example: babel.altavista.com

RSS Aggregators

RSS aggregators are websites that allow you to bookmark and read your favorite RSS feeds. RSS Aggregator sites will connect to the blocked websites and download the the RSS feed and make it available to you. Since it is the aggregator connecting to the website, not you, you will be able to access the censored content.

Example: www.bloglines.com

Alternate Domain Names

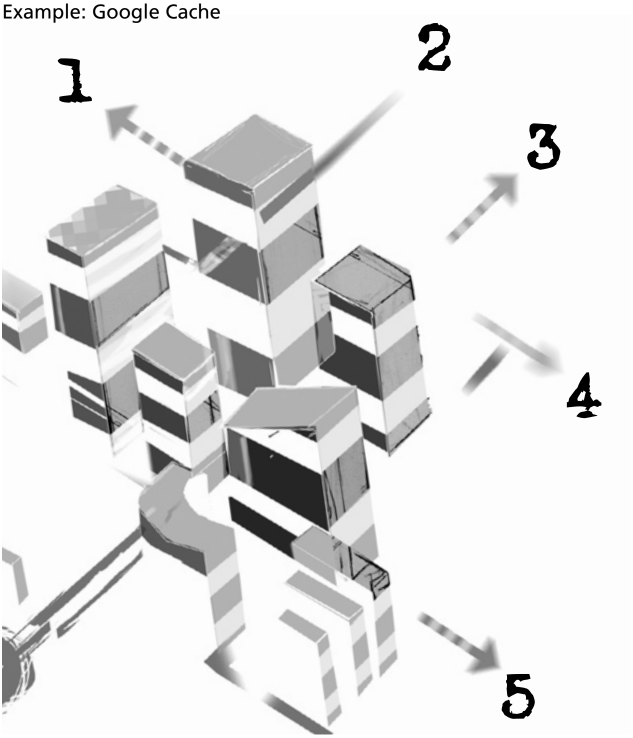
One of the most common ways to censor a website is to block access to its domain name, e.g. news.bbc.co.uk. However, sites are often accessible at other domain names such as newsrss.bbc.co.uk. Therefore if one domain name is blocked try to see if the content can be accessed at another domain.

Example:
news.bbc.co.uk ->
newsrss.bbc.co.uk

Web Accelerators

Web Accelerators cache web pages and make it appear as if your Internet connection is faster. Since you are retrieving the website from the cache and not from the blocked website directly, you can access censored content.

Example:
webaccelerator.google.com



things to remember

- There are a many ways to get access to a blocked site. Most methods do not allow you to do this securely. Find a method that provides you with both access and security.

- The more private your circumvention solution the better. Regardless of the choice of technology, private solutions stand the best chance of not being discovered and blocked.

- You increase your level of stable and secure circumvention if you are able to use a trusted out of country contact.

- Never use an out of country contact you do know and trust! Your contact can be your key to safety and your most important source of vulnerability.

- Remember that your provider can potentially see everything you are doing through a circumvention system.

- Violating state laws regarding Internet censorship can be a major risk. Do not use any technology you do not fully understand or know how to operate. Make a a thorough threat assessment based on your country context, skill level, and social network.

- Make sure to understand fully the technology you are using. Some services advertize security and anonymity, but do not actually provide them or require extra configuration or fees in order to activate such features.

further reading

NGO-in-A-Box **http://security.ngoinabox.org/**
A multi-lingual and peer reviewed collection of software and manuals to increase computer security and Internet privacy for human rights defenders and independent media.

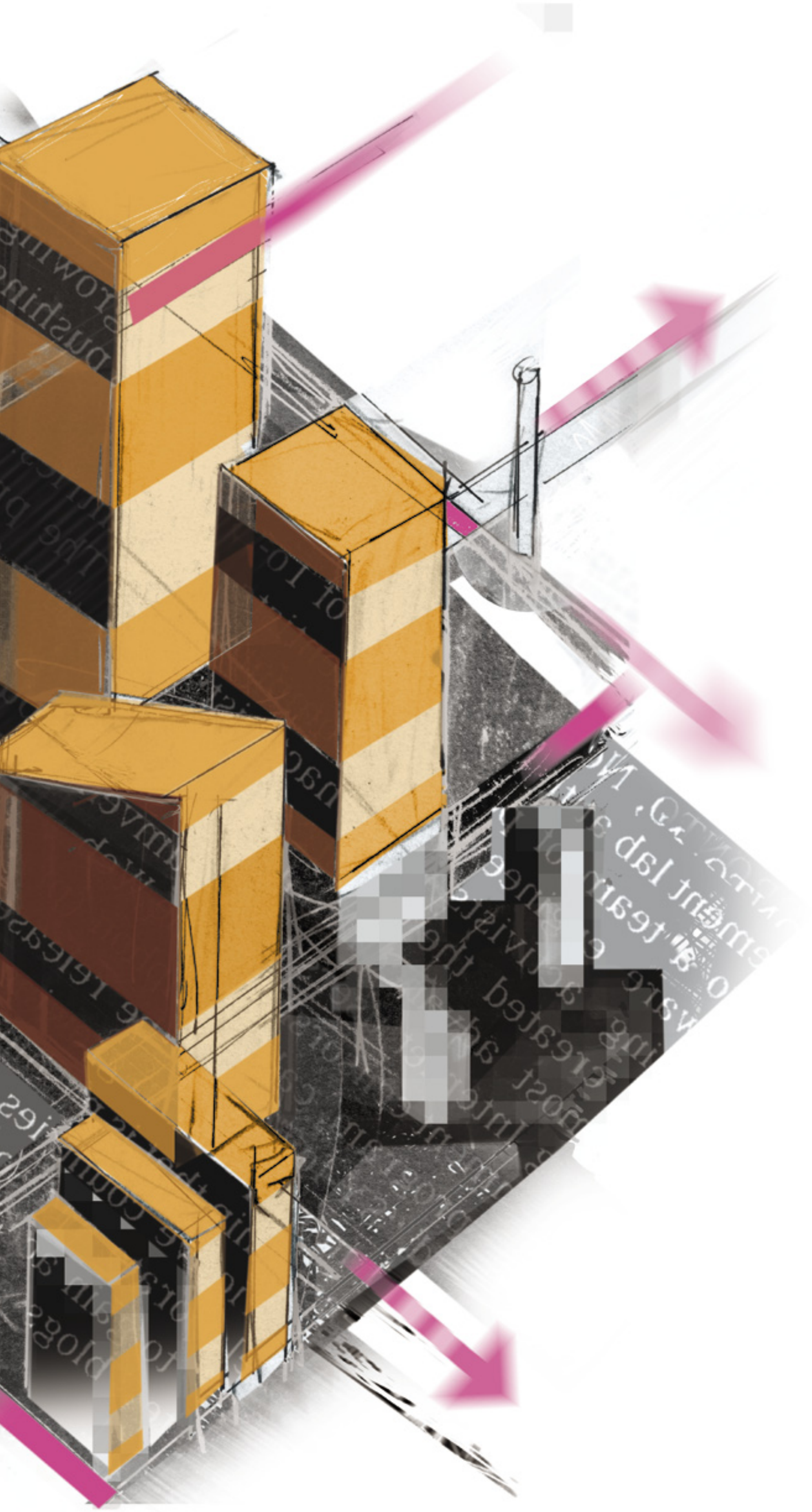
Tactical Technology Collective **http://www.tacticaltech.org/**
A non-profit foundation promoting the use of free and open source software for non-governmental organizations, and producers of the Security NGO-in-A-Box.

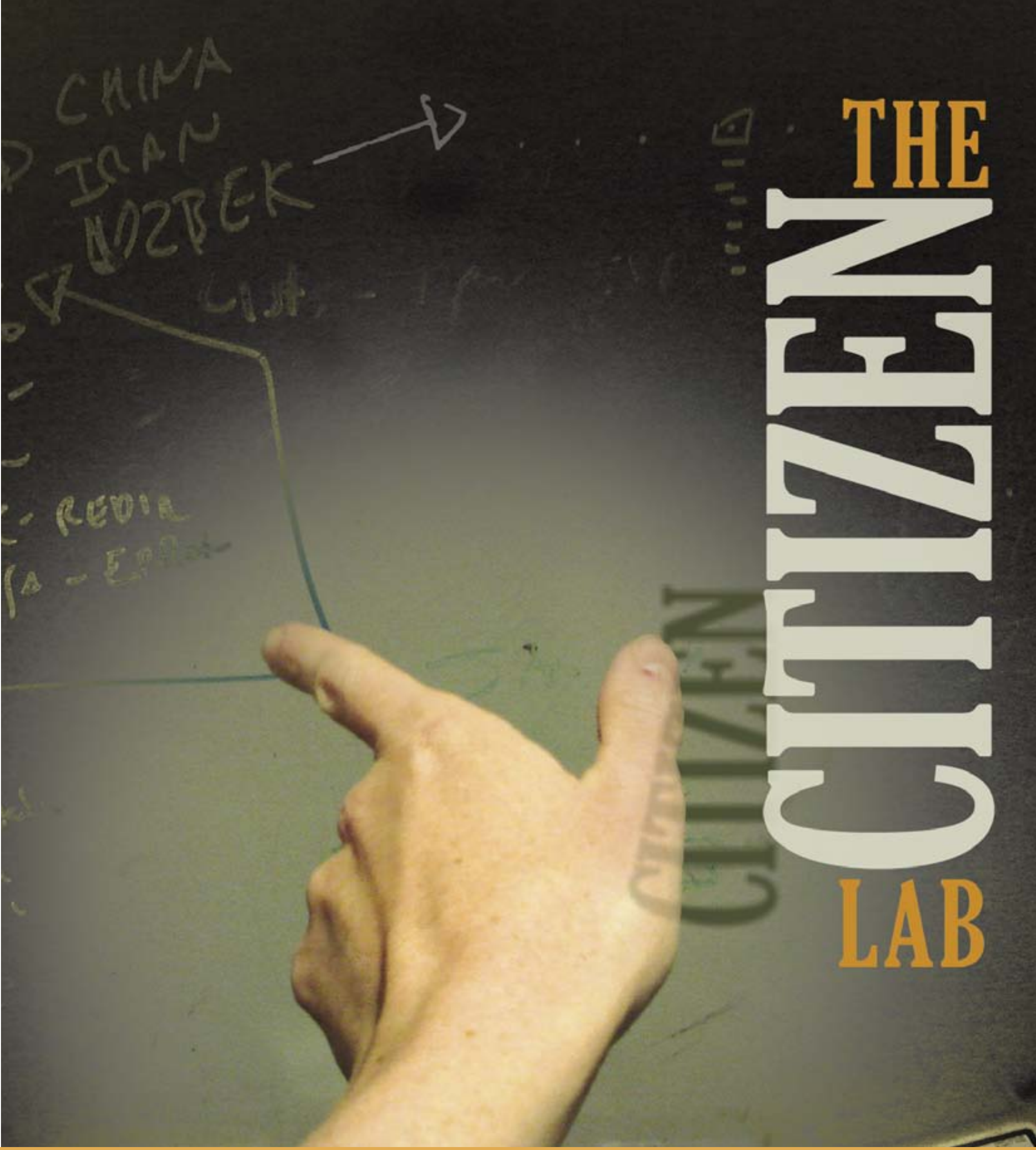
Reporters Without Borders, Handbook for Cyber-Dissidents and Bloggers
http://www.rsf.org/rubrique.php3?id_rubrique=542

OpenNet Initiative **http://opennet.net/**
A collaborative project among the Universities of Toronto, Cambridge, Oxford and Harvard whose aim is to document Internet censorship and surveillance worldwide.

Digital Security and Privacy for Human Rights Defenders
http://www.frontlinedefenders.org/manuals/en/esecman/
by Dmitri Vitaliev Published by Front Line - The International Foundation for the Protection of Human Rights Defenders.

ICE **www.nartv.org/blog/**
Blog of Citizen Lab Research Fellow, Nart Villeneuve.





www.citizenlab.org

University of Toronto
Munk Centre
for International Studies
at Trinity College

THE CITIZEN LAB is an interdisciplinary laboratory based at the Munk Centre for International Studies at the University of Toronto, Canada that engages in advanced research and development at the intersection of digital media and world civic politics.

A "hothouse" that brings together social scientists, computer scientists, activists, and artists, the Citizen Lab's projects explore the political and social dimensions of new information and communication technologies with a focus on human rights, humanitarianism, and democratic change worldwide.

The civisec project is sponsored by the generous support of the Open Society Institute.