

Leaping Over the Firewall:

A Review of **Censorship**
Circumvention Tools





Leaping Over the Firewall:

A Review of Censorship Circumvention Tools

Prepared by:

Cormac Callanan (Ireland)
Hein Dries-Ziekenheiner (Netherlands)
Alberto Escudero-Pascual (Sweden)
Robert Guerra (Canada)

This report has been prepared within the framework of Freedom House funding. The views expressed in this document do not necessarily reflect those of Freedom House.

Contacts

For further information please contact:

Mr. Cormac Callanan
Tel: +353 87 257 7791
Email: cormac.callanan@aconite.com

Mr. Hein Dries-Ziekenheiner
Tel: +31 71 711 3243
Email: hein@vigilo.nl

Mr. Alberto Escudero-Pascual
Tel: + 46 8 540 666 46
Email: aep@it46.se

Mr. Robert Guerra
Tel: +1 202 296 5101
Email: guerra@freedomhouse.org

The Authors

Cormac Callanan

Ireland

Cormac Callanan is director of Aconite Internet Solutions (www.aconite.com) which provides expertise in policy development in the area of cybercrime and internet security and safety.

Holding an MSc in Computer Science, he has over 25 years of working experience on international computer networks, and 10 years experience in the area of cybercrime. He has provided training at Interpol and Europol, and to law enforcement agencies around the world. He currently provides consultancy services around the world, and worked on policy development with the Council of Europe and the UNODC.

In 2008, he completed a study of best practice guidelines for the cooperation between service providers and law enforcement against cybercrime (www.coe.int/cybercrime). In 2009, he produced the 2Centre (Cybercrime Centres of Excellence Network for Training Research and Education) study profiling international best practice for IT forensics training to Law Enforcement (www.2centre.eu).

Cormac was president and CEO of INHOPE, the International Association of Internet Hotlines (www.inhope.org) coordinating the work of internet hotlines responding to illegal use and content on the internet. He co-authored the INHOPE first Global Internet Trend report in 2007, which was a landmark publication on internet child pornography. He was president of the board of the European Internet Service Providers Association (EuroISPA).

Hein Dries-Ziekenheiner

The Netherlands

Hein Dries-Ziekenheiner LL.M is the CEO of VIGILO consult, a Netherlands based consultancy specializing in internet enforcement, cybercrime, and IT law. Hein holds a master's degree in Dutch Civil law from Leiden University, and has more than ten years of legal and technical experience in forensic IT and law enforcement on the internet.

Hein was a technical advisor to the acclaimed Netherlands anti-spam team at OPTA and the Netherlands Independent Post and Telecommunications Authority, and frequently advises on both technical and legal issues related to cybercrime. He has provided training to law enforcement agencies around the world. He was responsible for the first-ever fine issued to a spammer under the EU anti-spam legislation while at OPTA; as lead investigator, he was involved in many cybercrime-related enforcement actions and takedowns, including several malware cases and high profile international spam cases.

Hein served as legal and regulatory counsel and representative of the Netherlands ISP Industry Association (NLIP) and delegate to the board of the European Internet Service Providers Association (EuroISPA).

He regularly presents and moderates technical training sessions at international conferences on cybercrime and security, and delivers training at both government and industry events. He currently serves as chair to the London Action Plan training committee.

Hein regularly publishes and speaks on issues relating to internet law enforcement and cybercrime. He has trained many law enforcement agencies in the use of the internet in their investigations.

Alberto Escudero-Pascual

Sweden

Alberto Escudero-Pascual obtained his doctorate in the area of computer security and privacy at the Royal Institute of Technology (KTH) in Sweden. His research focused on the technical, legal and social challenges of anonymity in the internet.

In 2004, Escudero started IT46 (<http://www.it46.se>), a consultancy company dedicated to the transfer of knowledge to promote social change.

Currently, IT46 participates in two open telephone and wireless projects: Freedom Fone (www.freedomfone.org)

and the Village Telco (www.villagetelco.org).

For the past ten years, Escudero serves as an independent expert for the European Commission, reviewing and monitoring the implementation of projects in the area of “Trust and Security.”

Robert Guerra

Canada

Robert Guerra heads the Global Internet Freedom Initiative at Freedom House. The initiative aims to analyze the state of internet freedom, to expand the use of anti-censorship technologies, to build support networks for citizens fighting against online repression, and to focus greater international attention on the growing threats to users’ rights.

Robert is also one of the founding directors of Privaterra, an ongoing project of the Tides Canada Foundation that works with nongovernmental organizations to assist them with issues of data privacy, secure communications, information security, internet governance, and internet freedom. He is often invited to speak at events to share the challenges being faced by social justice organizations in regards to internet freedom, surveillance, censorship, and privacy.

Robert Guerra was actively involved in the UN World Summit on the Information Society; he was an active member of its civil society bureau and internet governance caucus, and was the nongovernmental advisor to the official Canadian government delegation. He advises numerous nonprofits, foundations and international organizations, including Taking IT Global, DiploFoundation’s Internet Governance and Policy Capacity Building Programme, and the OpenNet Initiative.

Contents

Prologue	8	In-Country Survey Results	46
		Importance of Speed Versus Security	49
Executive Summary	9	Acquiring tools	49
Conclusions	11	Republic of Azerbaijan	50
Recommendations	11	Burma	52
		China	54
Introduction	13	Iran	56
The need for Internet Freedoms	13		
Report Methodology	15	Findings and Recommendations	59
Selecting the right tool	15	Findings	59
		Recommendations	60
Blocking and Censorship	18		
Introduction to phenomenon	18	Glossary	63
Technical methods used to block	19		
Technical methods used to circumvent	22	Appendix 1 Methodology	65
Possible actions against circumvention	23	Technical Assessment Methodology	65
		Survey Methodology	69
Circumvention Tools Technical Evaluation	27	Appendix II Survey Questionnaire	71
Summary	28		
Dynaweb	30		
Freemove	32		
GTunnel	33		
Gpass	34		
Google (Reader, Translation, Cache)	35		
Hotspot shield	36		
JAP	38		
Psiphon	40		
Tor	41		
Ultrasurf	43		
Your Freedom	44		

Prologue

Internet censorship poses a large and growing challenge to online freedom of expression around the world. Numerous countries filter online content to hinder the ability of their citizens to access and share information. In the face of this challenge, censorship circumvention tools are critical in bypassing restrictions on the internet, thereby protecting free expression online.

Freedom House conducted this product review to help internet users in selected internet-restricted environments assess a range of circumvention tools and choose the tools that are best suited to their needs. The product review determines how well different tools work in circumventing internet filters, and assesses each of the tools through surveys in the selected countries of Azerbaijan, Burma, China, and Iran. By providing this assessment, Freedom House seeks to make circumvention tools more accessible in countries where they are needed, thereby countering internet censorship. The evaluation is also useful for tools developers to learn how their tools are perceived by the users in these countries, and what enhancement would be beneficial. The tools selected for evaluation were chosen after consultation with users in these countries.

Freedom House would like to thank the report authors Cormac Callanan, Hein Dries-Ziekenheiner, and Alberto Escudero-Pascual (an independent expert in trust of security of the European Commission, Information Society) for the technical assessment of the tools as well as Arash Abadpour, Walid Al-Saqaf, Wojtek Bogusz, Fei Shen, and Jillian C. York for their constructive comments.

In addition, Freedom House would also like to thank our local collaborators who conducted the surveys in Azerbaijan, Burma, China, and Iran.

Overall guidance for the project was provided by Deputy Director of Programs Daniel Calingaert, Internet Freedom Project Director Robert Guerra, Caroline Nellemann, Lindsay Beck and Robert Getz.

This project was made possible by a grant from The US Department of State, Bureau of Democracy, Human Rights, and Labor.

If you have comments and questions regarding this report, Freedom House encourages you to contact us at [**internetfreedom@freedomhouse.org**](mailto:internetfreedom@freedomhouse.org).

The tools were analysed and the surveys conducted during March 2010.

David J. Kramer
Executive Director

Freedom House
Washington D.C.

Executive Summary

Internet censorship poses a large and growing challenge to online freedom of expression around the world. Censorship circumvention tools are critical to bypass restrictions on the internet and thereby to protect free expression online.

Circumvention tools are primarily designed to bypass internet filtering. Therefore, the core principle behind these technologies is to find alternative paths for data packets. These alternative paths use one or more collaborative servers in order to bypass the network of blocking mechanisms.

This document provides a comparison among different circumvention tools, both in terms of their technical merits, as well as how users of these tools describe their experience with them. The countries included in this report are Azerbaijan, Burma, China and Iran.

The preservation of human rights, and in particular the ones that could be in conflict with an internet blocking measure, i.e. the right to privacy or to freedom of expression, are often considered as intrinsic in democracy. Internet blocking systems operated by states can significantly interfere with their citizens' fundamental human rights. However, those who have determined to distribute such content on the internet have a myriad of options to do so, despite network blocking taking place. The primary objective of internet blocking is that internet users are prevented from receiving and viewing specifically-targeted content. Often, blocking systems prevent users inside one country from communicating with others outside of that country's borders.

Tools such as Herdict measure the extent of blocking in certain countries, and are extremely useful and widespread; adoption should be encouraged. Herdict Web aggregates reports of inaccessible sites, allowing users to compare data to see if inaccessibility is a shared problem.¹

Internet users looking to bypass such government censorship will be empowered in their ability to circumvent internet censorship by using this assessment of anti-censorship tools and methods. The product review is also an essential opportunity for technical developers to assess their products' strengths and weaknesses, and optimize the technical solutions.

This report focuses on blocks preventing the sending or receipt of specific content at a national level. This type of blocking is frequently employed in repressive regimes, whose primary purpose is to limit access to certain content that the regime deems politically or ethically undesirable. The technical infrastructure required for this is significant.

The strategies to disrupt circumvention tools include:

- ▶ **Technical measures to disrupt usage, prevent access to content, monitor usage, and where possible, identify the parties involved;**
- ▶ **Legal and self-regulatory measures to sanction circumvention or prevent distribution of tools;**
- ▶ **Propaganda promoting state-sponsored ideologies, which stimulate fear and uncertainty about the security of circumvention tools and exaggerate the effectiveness of monitoring and blocking systems in operation.**

The circumvention tools in this review were assessed in two ways. Firstly, each tool was technically evaluated based on the three categories of usability, performance, and support/security. The range of criteria was divided into these three categories so that the average internet user can understand and relate to the test result.

Second, using the same three categories, the country survey determined how the tools performed from a user's point of view, recognising that such tools are used in different countries under different internet blocking regimes. Different tools will be adopted by users in

1 www.herdirect.org/web.

different countries based on experience; expectations; privacy requirements; intuitive and technical information about blocking technologies in use; the urgency and types of communications; and the internet network architecture in each country. Users in Azerbaijan, Burma, China, and Iran were consulted.

Eleven tools (listed in the tools section) were evaluated, as were several widely available solutions such as VPN tunnels and proxy servers. Results of the evaluation are presented in easy-to-read tables showing how each of the tools performed from all the tests and surveys. Each tool is then described from a technical point of view. The Gpass, Psiphon, Tor, and the generic VPN category had very high results from the technical testing of security. For ease-of-use in terms of daily access to blocked websites for reading purposes, Google (specifically Reader, Translate, and Cache), UltraSurf, and Your Freedom were used widely.

Four countries are profiled in terms of the current state of their political system and their level of use of internet services. The highlights from the resulting in-country survey are listed for each country. The more affluent societies such as China and Iran consider home computers as a predominant access model, whereas the predominant access model in Azerbaijan and Burma is through internet cafes.

The survey of tools for each country displayed remarkable differences with the laboratory tests, mostly in terms of perceived security. Whereas the laboratory tests highlighted the lack of security when using tools such as Google, in-country users still perceived these tools as secure and well-supported.

Considering the environments in which these tools are used, a surprising result from the in-country surveys is that the user community generally selected a preference for speed of operation over security and anonymity of the communication. Choice of speed of operation over security is a complex decision. Doing things quickly can sometimes avoid detection. This depends on the level

of monitoring and logging on the network, since high levels of logging and monitoring will prevail over speed, putting users at greater risk. Speed is often a concern in low bandwidth locations, and as a result, users make a trade-off between speed and security. This might also be explained by minimal or absent enforcement towards those who wish to receive blocked content, whereas only a minority of users employ circumvention tools to transmit politically sensitive speech out of the jurisdiction. Unfortunately, it could indicate a serious lack of understanding on the nature of internet security by users in these regimes.

Key Survey Findings

- ▶ **Azerbaijan displayed a relatively low incidence of blocked content. Google was the leading tool from the survey, and is an understandable choice given reportedly slow internet access speeds and preference for usability. The internet community appear to rely on internet cafes to provide the required anonymity.**
- ▶ **Burma has a higher incidence of blocked content, and strictly limits free speech, which explains the almost equal appreciation of ease of use, performance, and security. The highest-ranking tool (a web based proxy system) for Burma does not provide a high level of security, however, probably due to the high use of internet Cafes. Installing circumvention tools is rarely easy in such locations.**
- ▶ **China has a well-developed internet infrastructure with increasing liberalization towards mass internet access. While comprehensive filtering is still present, this does not disrupt users too greatly, according to survey results. Freenet was the preferred tool here. Despite a complex, highly resourced blocking system, the results indicate that Chinese users are quite skilled in accessing blocked sites.²**

2 For example, see <http://www.guardian.co.uk/world/2011/feb/18/china-great-firewall-not-secure-internet>.

- **The favorite choice in Iran is a generic tool (VPN) that circumvents the very stringent blocking system, since most internet access takes place from home computers.**

Conclusions

The conclusions to be drawn from the in-country and technical testing is that there are a range of tools for a variety of internet blocking environments that can effectively circumvent internet blocking regimes. User knowledge is quite varied, and there is a concern that users seem to prioritise speed over safety and security. This is more dangerous for those who are sending material rather than those who are accessing and viewing material on the internet.

Most of the tools achieve high scores, and have delivered a high level of security and usability across the world. These tools need to continue to evolve to improve their reliability, and to overcome newer methods that block internet content. All of the tools need to invest efforts to ensure plausible deniability for users. Plausible deniability refers to the ability of tools to not easily be detected in use, and to leave minimal forensic footprints and evidence by users operating in dangerous environments.

Not every tool is equally suited for every user. This is due to differences in the censorship and blocking methods involved, and also due to the internet access methods and locations involved in the countries under investigation.

Recommendations

For Users:

- **It is strongly recommended that users carefully plan their internet access needs according to their internet usage and risk profile, and the nature of the regime they live under.**
- **Users need to be aware of other aspects of computer and network security to protect their activities online. It is important to remember that circumvention tools are not always designed with privacy and security in mind.**
- **Safety and security must become a way of life for activists who live in repressive regimes.**

For Tools Developers:

Usable solutions are not only those that perform functional tasks, but are also able to educate users about their options when selecting one type of tool over another.

- **Usable solutions are those that have training materials and community support forums, and have access to a well-designed user interface.**
- **Privacy and confidentiality regarding the use of circumvention technologies creates substantial technical challenges that deserve further research and investment.**

Future Work

- **Regular, repeated testing of these tools, both in-country (where feasible), and in technical lab environments, is essential.**
- **Greater thought should be given to a more user-centric manual or security guide that provides more comprehensive information to users with restricted internet freedom.**
- **Greater attention should be given to the attitudes and requirements of internet users living under oppressive regimes.**

Introduction



Introduction

The need for Internet Freedoms

Internet restrictions fundamentally limit freedom of expression online.³ Tools that empower personal privacy and improve ways of accessing public information and of publishing information are widely available. Tools that directly disrupt deliberate attempts to prevent free online communication through the use of internet blocking systems are called circumvention tools. Such tools play a great role in countering internet restrictions, whether the barriers involve accessing information, uploading content, or communicating with others online.

During her remarks at the Newseum in Washington in January 2010, U.S. Secretary of State Hillary Rodham Clinton stated that “the spread of information networks is forming a new nervous system for our planet. When something happens in Haiti or Hunan, the rest of us learn about it in real time—from real people. And we can respond in real time as well. During his visit to China in November, for example, President Obama held a town hall meeting with an online component to highlight the importance of the internet. In response to a question that was sent in over the internet, he defended the right of people to freely access information, and said that the more freely information flows, the stronger societies become. He spoke about how access to information helps citizens hold their own governments accountable, generates new ideas, and encourages creativity and entrepreneurship.”⁴

Secretary Clinton went on to say that “technologies with the potential to open up access to government and promote transparency can also be hijacked by governments to crush dissent and deny human rights. In the last year, we’ve seen a spike in threats to the free

flow of information. China, Tunisia, and Uzbekistan have stepped up their censorship of the internet. Some countries have erected electronic barriers that prevent their people from accessing portions of the world’s networks. They’ve expunged words, names, and phrases from search engine results. They have violated the privacy of citizens who engage in non-violent political speech. These actions contravene the Universal Declaration on Human Rights, which tells us that all people have the right “to seek, receive and impart information and ideas through any media and regardless of frontiers.” With the spread of these restrictive practices, a new information curtain is descending across much of the world. And beyond this partition, viral videos and blog posts are becoming the samizdat of our day.”⁵

According to the members of the European Parliament, unimpeded access to the internet without interference is a right of considerable importance. The internet is “a vast platform for cultural expression, access to knowledge, and democratic participation in European creativity, bringing generations together through the information society,”⁶ and is protected by the right to freedom of expression, even when it is not currently considered as a fundamental right in itself.

In recent years, some democratic states have also promoted the use of internet blocking technologies in relation to a variety of narrowly specified types of content. They cite public demand for specific blocks, even though the very characteristics of the internet cause enforcement issues. These subject matters vary from the availability of Nazi memorabilia via online marketplaces, to gambling websites hosted in countries with liberal regimes in relation to online gambling. However, in stark contrast, states with significantly less open information regimes with little regard for human rights have adopted wide-scale internet blocking as

3 Similar restrictions exist in many countries to various degrees with the significant exception that they are narrowly targeting specific types of illegal content.

4 Hillary Rodham Clinton, US Secretary of State, The Newseum, Washington, DC, January 21, 2010. Available at <http://www.state.gov/secretary/rm/2010/01/135519.htm>.

5 Clinton, January 21, 2010 speech.

6 European Parliament resolution of April 10, 2008 on cultural industries in Europe, 2007/2153(INI), § 23, accessible at this address: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2008-0123+0+DOC+XML+V0//EN>.

a technical resource for extending their practice of information control into the online world.⁷

Internet blocking systems as operated by the state can significantly interfere with a citizen's fundamental rights.

It is important to note the intrusive nature of many blocking strategies. This is especially true for the more granular, content-based filtering mechanisms that require insight into the content of the material being exchanged among individual users. This is not only problematic from an investment perspective (the required investment is invariably high in these scenarios) but also from a broader, societal point of view.

This report offers a technical review of eleven different tools and methods and a practical methodology to evaluate them. The review aims to make accessible an area of knowledge for those interested in circumvention, but do not necessarily have the resources or skills needed to research the large volume of documentation on available circumvention tools and techniques. Furthermore, this report tries to eliminate the need for familiarity with the purely technical aspects of filtering and circumvention technologies, which are highly sophisticated technological endeavours.

The reader of this report is also saved from having to allocate resources for installing the tools in order to choose the one that fits their usage pattern. In addition to the technical review, results of the user surveys on the eleven circumvention tools are presented. These subjective experiences will complement the purely technical descriptions of the tools described in this document.

The circumvention tools and methods are assessed under three general categories of usability; privacy and security; and transparency and sustainability. The

ranking of the tools shows how well these tools operate, and thereby highlights the strengths and weaknesses of each tool. While some features of a tool can be applied universally, other features only work in particular situations. Illustrating the effectiveness of the tools according to the criteria allows internet users to identify the tool or tools that will work best for them.

The report begins by introducing the methodology used for both technical testing and conducting the user surveys. The methodology is followed by an assessment and rating of each of the eleven tools based on the technical testing as well as feedback from internet users, presented in a series of country summaries. The technical assessment is complemented by the in-country surveys that were conducted. These surveys collected views of the users about the tools and their experiences. The results of these surveys are described for each country. The findings are then summarized, and a set of recommendations is presented. In addition, a section describing the technical testing environment, as well as a glossary explaining some of the technical terms that are frequently used in this review, are included in the appendix.

For example, one surprising key result from the in-country surveys was that the user community generally selected a preference for speed of operation, over security and anonymity of the communication. It is surprising that users would prioritize their ability to quickly access and send information through blocking systems above their own personal safety and security. Unlike real-world environments, speed of activity on the internet is not a challenge for blocking and monitoring systems that can analyse, collect, and report on data connections, regardless of the speed of transmission. Users might chose speed in order to sacrifice their own safety to ensure that an important message is transmitted or received, or users might do so out of ignorance of the risks taken. It is important that such decisions are made with the support of assessments conducted in this report.

7 Study on Internet blocking - balancing cybercrime responses in democratic societies" by Cormac Callanan (Ireland), Marco Gercke (Germany), Estelle De Marco (France), Hein Dries-Ziekenheiner (Netherlands). October 2009. www.aconite.com.

The Tor Project published a comprehensive article in September 2010, entitled “Ten Things to Look for in a Circumvention Tool.”⁸ It confirms that circumvention tools provide different features and levels of security, and it is important for users to understand the complex tradeoffs.

By using this report and the assessment of the anti-censorship tools and methods, internet users will be empowered in their ability to circumvent internet censorship. Additionally, the product review will be an important tool for technical developers in assessing their products’ strengths and weaknesses, and optimizing the technical solutions.

Report Methodology

This report presents the result of a comparative review of the most popular initiatives in the area of internet blocking circumvention tools. The authors are aware that comparing different technologies and projects is a very complex task. In order to increase the objectivity of this exercise, a comprehensive methodology was developed and adopted. This methodology included a technical evaluation in a laboratory setting, supported by in-country surveys.

The user surveys in the target countries are all based on the same set of questions that were initially developed in English. The surveys were then distributed in each target country, although it was not possible to achieve a rigorous survey sampling due to the repressive nature of the regimes in those countries. The purpose of the survey, therefore, is to determine how the tools perform from a user’s point of view, recognising that such tools are used in different countries under different internet blocking regimes. Different tools are adopted by users in different countries based on experience; expectations; privacy requirements; access to technical gossip on popular blocking technologies in use; the urgency and types of communications; and the internet network architectures in each country.

Detailed information on the methodology used is available in Appendix II.

Selecting the right tool

Selecting the right tool to circumvent internet blocking is an important decision that should be undertaken after careful reflection. The following flowchart is designed to support the decision-making process in the selection of the appropriate tool. The tools selected are based on the laboratory testing component, and excludes the in-country surveys.

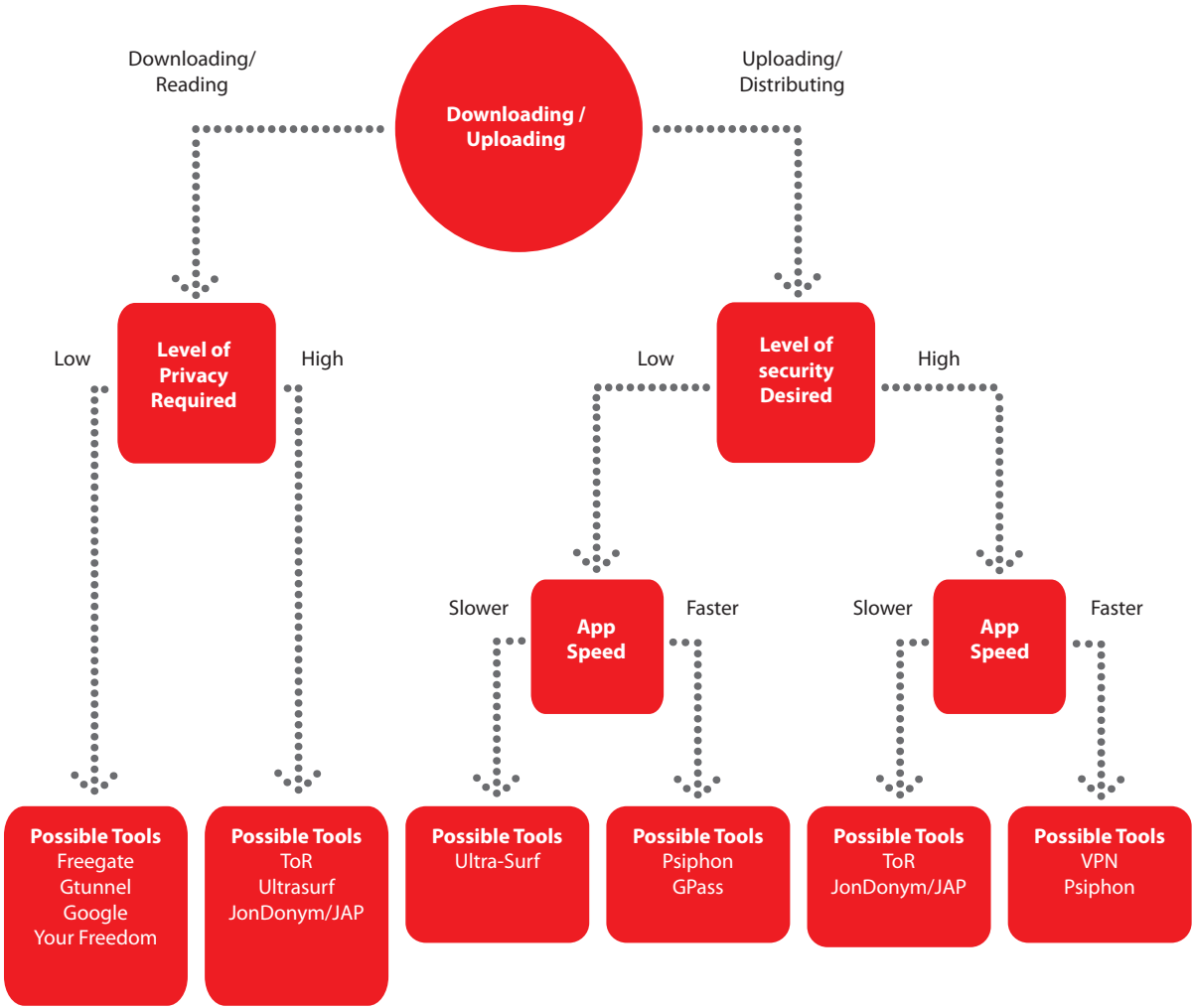
It is important to elaborate on the meaning of security and anonymity.⁹ The clear conclusion is that circumvention does not offer guarantees of security in terms of confidentiality.¹⁰ Privacy regarding the use of the technology is a technical challenge that is a significant issue for all users. Circumvention tools need to offer technical mechanisms to conceal the fact that circumvention technology is in use. Privacy and circumvention tools do not necessary go hand in hand. Users should be informed about the personal information that is provided to the operator of the circumvention technology infrastructure.

8 <https://www.torproject.org/press/presskit/2010-09-16-circumvention-features.pdf>.

9 An important concept to remember about anonymity is the ability to not to be easily identifiable in a crowd. Anonymity depends on how large the crowd is around you, or how similar you are to others

10 Confidentiality is to ensure that information is available only to those authorized.

Simplified Flowchart providing guidelines on how to select the appropriate tool



Speed is a complex decision. Doing things fast can sometimes avoid detection. This depends on the level of monitoring and logging on the network since high levels of logging and monitoring will prevail over speed.

Blocking and Censorship



Blocking and Censorship

The development and implementation of various types of internet blocking technology on the internet is not a recent development. For a long time, spam, internet-based viruses and malware, and many other content-types that are unwanted or unrequested by users, have been targets of blocking efforts undertaken by industry for security and usability reasons, or by the state in its role as a developer and enforcer of laws and policies.

A technical overview of the major internet blocking systems in use today is essential, as is an explanation on how these are applied to different internet services. In addition to concerns about the effectiveness of such blocking systems, there are also significant technical impacts and challenges created by these systems. There are also many ways to evade these blocking systems, and a brief overview of the effectiveness of these systems is included here.

The resources and continuous effort required to constantly evade blocking activities while remaining anonymous should not be underestimated. On the one hand, it is likely that mistakes will occasionally occur. On the other hand, it is important to note that the resources and efforts necessary to create and maintain an internet blocking system are significant. To ensure the continued effectiveness of national blocking systems, states are required to commit substantial resources to constantly respond to these evasive activities, in order to develop additional technical responses. For example, the Guardian newspaper reported that Dr. Fang Binxing, an architect of the Chinese “Great Firewall,” told a Chinese newspaper there was a constant battle between the apparatus and technologies such as virtual private networks (VPNs), which allow users to “climb the wall” and look at banned sites. “So far, the GFW [Great Firewall] is lagging behind and still needs improvement,” said the man known as its developer. Further tightening is needed to halt attempts to overcome its controls.¹¹

Introduction to phenomenon

Internet blocking has been around for many years. However, the term covers such a broad range of policies, hardware, software, and services that it would be a mistake to think that all types of internet blocking are the same; are equally effective; are legally equivalent; or even that one system can easily be used in relation to more than one type of content.

The primary objective of internet blocking is to block content from reaching a personal computer or computer display with a software or hardware product that reviews all internet communications and determines whether to prevent the receipt and/or display of specifically targeted content. Blocking can also be targeted at specific types of communication channels, such as blocking all voice-over-ip (voip) products, or blocking the use of peer-to-peer (p2p) software.

Problems with internet blocking systems become more pronounced and have greater impact when internet blocking systems are applied to the public internet at a national level, and are applied universally to all internet users in an area or entire country. These systems require that all internet intermediaries, including access providers, hosting providers, and service providers, all comply with the blocking and monitoring systems. This can be very problematic for commercial organisations, which are then constrained and hampered in their creativity. It also limits the complexity of the services they can provide, since they are required to ensure that any service designs abide by the complex blocking and monitoring requirements imposed by the government.¹² Since internet content can be exchanged over several internet technologies, the practice of blocking only a limited number of these technologies (such as blocking only traffic to web-servers) may also easily cause substitution of an alternative content distribution method.

11 <http://www.guardian.co.uk/world/2011/feb/18/china-great-firewall-not-secure-internet>.

12 See *Intermediary Liability: Protecting Internet Platforms for Expression and Innovation* <http://www.cdt.org/paper/intermediary-liability-protecting-internet-platforms-expression-and-innovation>.

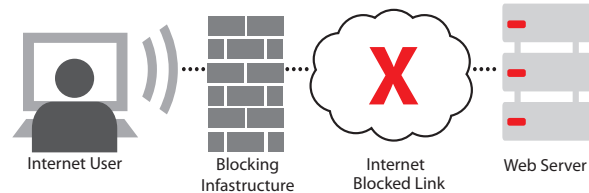
The internet is a vast, complex network of networks with a myriad of hardware systems, protocols, and services. The first step with an internet blocking initiative is to select where blocking can be attempted on the internet. In the case of the regimes that are the subject of this report, a second key concern is to determine who chooses the content to be blocked, and to determine the various skills and knowledge of different users and organisations in order to block “inappropriate” internet content.

Technical methods used to block

From a technical perspective, blocking can be performed in many different ways.

The most important characteristic is the technical level of the blocking that is taking place. In many daily internet applications, there is blocking functionality present for a variety of purposes. Examples of these are email services that have spam blocking capabilities, and child pornography blocking lists that are employed by service providers in various countries. In democratic societies, there is generally only a limited need to circumvent this type of blocking. Many of the systems reviewed in this report would not easily enable circumvention of blocking systems for illegal purposes, since many international servers can still record usage in logs for authorized review by law enforcement officers.

For the purpose of this report, the focus is on blocks that prevent the sending or receiving of specific content at a national level. This type of blocking is frequently employed in repressive regimes, whose primary purpose is to limit access to certain content that the regime deems politically undesirable. The technical infrastructure required for this is significant. A functional diagram representing such a blocking infrastructure is as follows:



There are significant differences in the blocking schemes of the countries studied in this report. The fact, however, that the central government seeks control of the characteristics of the block generally means that a central blocking list or set of criteria is present. In some countries, the application of such a list is enacted by centralizing the infrastructure so that all internet access takes place through government controlled networks or central nodes. In other countries, the block is implemented by imposing requirements on all ISPs offering service in the country.

Either way, an ISP or government implemented blocking system will need to be supplied with characteristics (such as keywords or internet addresses) of the content to be blocked. When such a characteristic is found, the block is implemented and the content is made inaccessible. At the same time, details that could identify the user attempting to access the content are often logged by authorities for later analysis and, in some cases, prosecution.

In general, there are four different targets that blocks could focus on:

- **Service-based approach (e.g. email, web, p2p, SNS);**
- **Content-based approach (e.g. hate-speech, child pornography, gambling websites, political opposition sites, human rights organizations, independent news sites, etc.);**
- **User-based activities (e.g. users who download illegal music; send spam; or, in repressive countries, advocate for human rights).**

- **Search engine-based approach (e.g. preventing search results for specific websites).**¹³

Specifying content

In order to attempt to block content, identifiers are needed whereby a blocking decision can be implemented. Current blocking methods have a number of options.¹⁴

- **IP Addresses** - Typically every computer that is connected to the internet has an IP address that uniquely identifies the machine and its user(s). Blocking an IP address means that other internet services and users that use the same address will also be blocked.
- **Port or Protocol** – Every computer that connects to an IP address connects from a certain port number to a certain port number. These numbers either identify separate connections, or (when services are offered at the IP address) a certain service or protocol. By convention, port 80, for instance, is used to identify a web-server that serves website content. If a specific port is blocked on an outgoing connection (e.g., port 80) this may hinder or block usage of services that rely on that port number.
- **Domain Names** - A domain name is used to identify a specific website, and enables linking a name to an IP address, and vice versa. It is important to understand that multiple domain names may be present on a single IP address, so blocking by a domain name will block all content residing under that domain.
- **Uniform Resource Locators (URL's)** – URLs are specific addresses inside a website or internet application (e.g. <http://www.hrw.org/zh-hans>). They specify the website content to be displayed or accessed in greater detail (in this case, a Chinese section of the Human Rights Watch website). Best results in terms of specificity will be obtained by filtering on a URL basis. Due to the ease of evading these filters, blocking by this identifier can lead to a significant risk of under-blocking.
- **Content Signatures** - Using signatures or some other representation of the data being accessed,¹⁵ content can be blocked with signatures that allow for classification of content that has been deemed illegal. New content is easily missed by these types of filters, however. Encryption of the content renders this method useless.
- **Keywords** – Keyword blocking is a specific form of signature-based blocking. It is based on keywords found either in the file name, the URL, or the text at the location of the content being accessed. Complex analysis of the recognised keywords in the context of their use must to be performed.

13 This could be eliminated when using SSL-supported search engines (like <https://encrypted.google.com>).

14 Compare, also, Internet Filtering: The Politics and Mechanisms of Control, Jonathan Zittrain and John Palfrey available at: http://akgul.bcc.bilkent.edu.tr/Yasak/Deibert_03_Ch02_029-056.pdf. See "Study on Internet blocking - balancing cybercrime responses in democratic societies" by Cormac Callanan (Ireland), Marco Gercke (Germany), Estelle De Marco (France), Hein Dries-Ziekenheiner (Netherlands). October 2009. www.aconite.com.

15 Typically hash values are used to generate signatures. Hashes are the result of cryptographic algorithms that allow for calculating a unique value for a specific set of data.

Blocking Summary¹⁶

This table lists characteristics of every blocking strategy discussed. It shows the likelihood of over and under-blocking according to our estimates; lists the resources required to execute the blocking strategy; identifies the block list type and maintenance efforts required for such a list; and indicates whether the communications content must be analysed extensively for this strategy (DPI technology or alike) to be effective. This is a good indication of how invasive this blocking method is.

Medium	Blocking	Effectiveness				Blocklist		DPI
		OVER-blocking	UNDER-blocking	Resources required	Circumvention	Maintenance effort	Identifier	
Web	DNS	Very Likely	Likely	Low	Easy	Medium	Domainname	-
	Domain	Very Likely	Likely	Medium	Medium	Medium	IP address to domainname	-
	URL	Less Likely	Very Likely	Medium	Medium	High	URL	+
	IP	Very Likely	Likely	Low	Medium	Medium	IP address	-
	Dynamic	Very Likely	Very Likely	High	Medium	Low	Keywords, graphics recognition technology or other	+
	Signatures	Less Likely	Very Likely	High	Medium	High	Hash	+
	Hybrid (IP+signature/URL)	Less Likely	Very Likely	Medium	Medium	High	Ip and Hash or URL	+

16 Study on Internet blocking - balancing cybercrime responses in democratic societies" by Cormac Callanan (Ireland), Marco Gercke (Germany), Estelle De Marco (France), Hein Dries-Ziekenheiner (Netherlands). October 2009. www.aconite.com.

Technical methods used to circumvent

Blocking web traffic effectively, (i.e., blocking the access of the user to the content and not merely using DNS filters) requires significant investment in proxy deep packet inspection infrastructure and substantial interception of all internet communications.

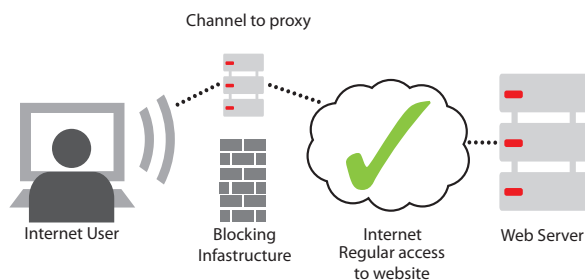
► Proxies

Circumventing internet blocking that prevents direct access to a foreign based website is quite simple. To circumvent a filter blocking access directly, a user can ask a foreign proxy to access the blocked content on his or her behalf. As long as that foreign proxy itself is not being blocked, the user can then gain access to the content to bypass local filtering.

A disadvantage of proxies is that the application that the internet user wishes to use (such as a browser or email program) must be “proxy aware”: it should have the option to set a proxy as an intermediary access server.

This approach also requires that the channel to the proxy not be blocked itself. To make interception of the information harder, all tools we tested also encrypted the traffic to the proxy. For a regular proxy this is not standard practise, but is generally supported by proxy protocols.

A diagram displaying a proxy server used to access content, despite blocking, is as follows:



Although most proxy servers speak a purpose-built proxy protocol, certain proxies can be accessed by more common protocols, such as secure https connections. In this case, the proxy acts as a web server, displaying content available from elsewhere on the internet.

► Tunneling / VPN

Tunnelling software allows users to create an encrypted “tunnel” to a different machine on the internet that prevents the filtering software from seeing web requests. Once a tunnel is created to the other machine, all internet requests are passed through the tunnel, to the machine on the other side, and then to the internet.

The access method is similar to the use of a proxy, except that a tunnel is recognized by the operating system as a separate internet connection: this means that it is possible to use tunnels without a specific setting in the application.

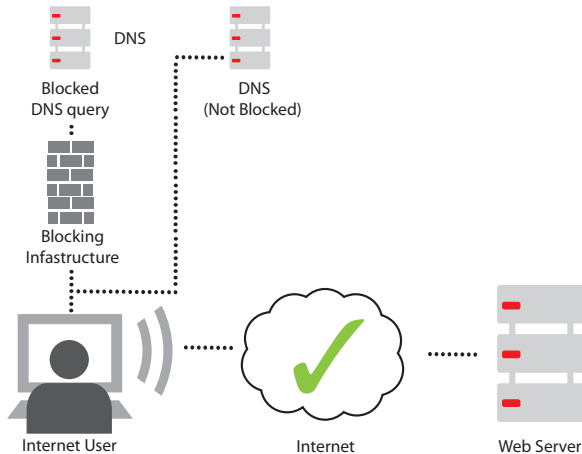
VPN tunnels are invariably encrypted and thus not susceptible to snooping (interception of traffic).

► DNS-based filters

DNS-based filters rely on a translation mechanism that translates the domain name of a site or resource to an IP address.

DNS-based filters are easy to bypass, as long as the internet connection to the blocked website or resource itself is not blocked. Merely changing the DNS server of the provider to a different one (which is not part of the blocking system) or (frequently) using the IP address of the remote website is enough¹⁷ to completely circumvent this blocking method.

17 Whether this works depends on whether a http- host: statement is required to access the website. Many sites operate on virtual hosting servers with shared IP addresses where direct IP access rarely works.



► Telescopic crypto (onion routing)

Telescopic cryptography or “onion routing” uses advanced public key encryption. A private key is available to its user only and is used for decrypting. The related public key, however, can safely be shared with the rest of the world and can encrypt communications destined for the private key holder. Only with the private key can encrypted data then be decrypted.

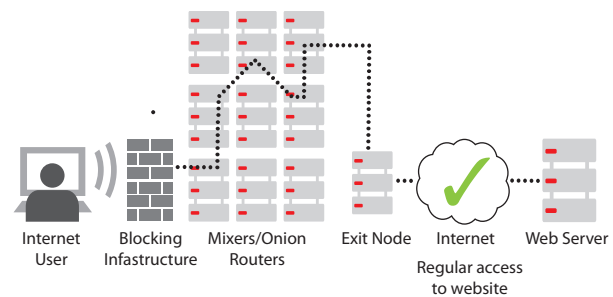
Using this technology, traffic being sent is encrypted with pre-shared public keys of servers (often called onion routers or mixers) and transmitted to them. It is decrypted once received (often through several stages, passing several routers or mixers along the way) until it reaches the final (exit) node on the network. From that point on, plain, decrypted traffic to the open internet is provided.

Using this principle makes it possible to employ layered cryptographic safeguards on tunnelled traffic (hence the reference to an onion or a telescope: every cryptographic layer needs to be peeled off before plain text traffic is visible at the exit-node).

A common combination for circumvention tools is to create a local proxy for local applications to use. Traffic sent to this proxy is then tunnelled to a server

outside of the regimes reach, and from there sent to the public, “free world” internet.

A representation of traffic flowing to a webserver through three onion routers and an exit node is as follows:



Possible actions against circumvention

There are many strategies that could be adopted to combat circumvention tools. The success of each strategy lies in the resources, skills, and experience of either party adopting or disrupting the use of circumvention tools.

The strategies can be grouped into several key areas:

- **Technical measures to disrupt usage, prevent access to circumvention tools, monitor usage and, where possible, identify the parties involved;**
- **Legal and self-regulatory measures to sanction circumvention or prevent distribution of tools;**
- **Propaganda to promote state-sponsored ideologies, stimulating fear and uncertainty about the security of circumvention tools, and exaggerating the effectiveness of monitoring and blocking systems in operation.**

Technical Measures against Circumvention

The technical measures are designed and implemented to block access to circumvention tools; promote access to content favourable to state-sponsored ideologies; and profile users of circumvention tools to distinguish users who seek, read and disseminate unauthorized content, from those who create unauthorised content, distribute unauthorized content, or leak confidential or otherwise privileged information.

Once such profiling begins, long-term collection and review from public intelligence sources can provide a range of data and information about the online activities of internet users in each country. Automated profiling may provide a range of data that permits heuristic analysis, and waits for any potential minor user mistakes to directly identify and target specific individuals. This direct identification is unlikely to occur using technical tools alone, and will usually require complex combinations of technology, monitoring, social engineering, and on-the-ground monitoring and human agents.

For example, social engineering can be used to encourage activists to unknowingly disclose technical data that could be used to trace connections on the internet to specific users. This could include permitting targeted cookies or specific images; or identifying files or inappropriate code to be downloaded to the activist's computer regardless of the safety of the communications methods used to obscure internet logs. These files can then be searched if and when access to the activist's computer is later obtained. Social engineering can also be used to compromise and access data stored online, including lists of contacts in Twitter, Facebook, etc.; and to facilitate a complete analysis and disruption of an entire network of users.

Considering the sizeable effort required by states to restrict internet activities, anti-circumvention strategies

are likely to be focused on those users producing and disseminating content, rather than the mass of users merely accessing prohibited information.

Internet malware can be developed and installed by governments to attack, monitor, or disrupt dissident computer systems and communication. Malware covers a broad spectrum of attacks against computer system integrity. It is important to note that malware that is specifically targeted at a regional, racial, or language group is very difficult to intercept and identify by any anti-malware products available today.¹⁸ For example, it would be possible for regimes to create confusion and provoke fear in users by distributing a range of fake circumvention tools under established names.

Legal and Self-Regulatory Measures

The legal and self-regulatory procedures are designed to enable states to implement broad spectrum monitoring and sanctioning of internet activists. The legislation usually directly penalizes activist behaviour; limits freedoms; and encourages a climate of regulatory confusion and uncertainty that serve to reduce the effectiveness of activists' messages and discourage others from participating in such behaviour. It is worth noting that internet control and blocking measures are more effective if the range of content being blocked is extremely narrow and/or the range of patrons circumventing such control systems is small. Therefore, from the state's point of view, a great deal of effectiveness can be achieved by taking steps to reduce these numbers.

¹⁸ According to Microsoft, the malware ecosystem has moved away from highly visible threats, like self-replicating worms, toward less visible threats that rely more on social engineering. This shift means that the spread and effectiveness of malware have become more dependent on language and cultural factors. Some threats are spread using techniques that target people who speak a particular language or who use services that are local to a particular geographic region. - Microsoft Security Intelligence Report, Volume 7, January through June 2009 <http://www.microsoft.com/sir>.

Propaganda Measures

Propaganda efforts seek to promote the state ideology in order to create a climate of fear in users and activists who strive to change such systems. They also stimulate rejection by other users who might be tempted to participate as conscientious objectors to support more freedoms and public discourse and debate.

Propaganda will also encourage the belief of the infallibility of the blocking systems and the complexity, technological capabilities, and resources available to the state agencies responsible for implementing blocking systems.

It will also strive to undermine confidence in tools designed to circumvent blocking systems by highlighting weaknesses, whether real, imaginary, or deliberately misleading in order to intentionally drive users towards weaker tools and processes. These weaknesses include alleged or real weaknesses in software design; in installation and configuration; and in encryption-algorithm design and implementation. Often these controversies are combined with the conviction of activists who, it will be suggested, used these weak tools. While this may sometimes be the case, detailed evidence of such use is not often disclosed and thus independent analysis of the evidence is not possible.

Conclusion

All of these methods are used to combat circumvention tools, and it is therefore important that these tools are regularly checked, updated, and tested. It is critical that users gain a broad understanding of the challenges facing them; understand and collect data on the blocking system in use in their country; perform regular analysis of the activities they conduct online; and audit the security and privacy of both their own online activities and also their local computer systems. Users should also be aware of the constant efforts that states make to track and trace their online activity. This effort may involve technical measures, but has also increasingly involved social engineering. This means that users should not only look at the technical angle of their approach, but should also be aware of frequent attempts to infiltrate or otherwise identify social networks of people with dissenting opinions, even when they are only partially operating online.

Circumvention Tools Technical Evaluation



Circumvention Tools Technical Evaluation

This section contains a list of the tools included in this investigation, including:

- Dynaweb
- Freerate
- GTunnel
- GPass
- Google (Reader, Translation, Cache)
- Hotspot Shield
- Jap
- Psiphon
- Tor
- Your Freedom
- UltraSurf

Summary¹⁹

Summary table: Results from technical lab testing alone

Description	Ease of Use	Performance	Support & Security	Average	Rank
Psiphon	★★★★	★★★★★	★★★★	★★★★	1
Gpass	★★★★	★★★★	★★★★★	★★★★	1
Tor	★★★★	★★★★	★★★★	★★★★	3
Ultrasurf	★★★★	★★★★	★★★★	★★★★	4
Google	★★★★	★★★★	★★★	★★★★	5
VPN	★★★★	★★★	★★★	★★★★	5
Gtunnel	★★★	★★★★	★★★★	★★★★	7
Dynaweb	★★★	★★★★	★★★	★★★★	8
JonDonym/JAP	★★★★	★★★★	★★★	★★★	9
Proxy	★★★★	★★★★	★★★	★★★	10
Your Freedom	★★★★	★★★★	★★★	★★★	10
Freagate	★★★★	★★★★	★★★	★★★	12
Hotspot shield	★★★	★★★	★★	★★★	13

The results of the summary are very encouraging. As a result of comprehensive testing, most tools scored three or more stars, and only one was questionable.

¹⁹ The scoring for each tool is determined by averaging the scores for all three categories (which are in turn calculated from a range of items as outlined in the methodology). The stars are allocated based on these scores – which have a two decimal accuracy. Hence, even where tools show the same number of stars, the final detailed score can vary - creating a specific tool ranking as indicated in the Rank column. For example a tool with an average of 2.5 stars will rank lower than a tool averaging 3.2. Both will have three stars, however.

**Summary table: Results from technical lab testing
combined with in-country surveys**

Tool		Laboratory Testing			In-Country Surveys			Overall Score	Rank
		Ease of Use	Performance	Support & Security	Ease of Use	Performance	Support & Security		
1	Google	★★★★	★★★★	★★★	★★★★	★★★★	★★★★	★★★★	1
2	Psiphon	★★★★	★★★★★	★★★★	★★★★	★★★★	★★★	★★★★	2
3	Gpass	★★★★	★★★★	★★★★★	★★★★	★★★★	★★	★★★★	3
4	VPN	★★★★	★★★	★★★	★★★★	★★★★	★★★	★★★★	4
5	Ultrasurf	★★★★	★★★★	★★★★	★★★★	★★★★	★★★	★★★★	5
6	Tor	★★★★	★★★★	★★★★	★★★	★★★★	★★	★★★★	6
7	Proxy	★★★★	★★★★	★★★	★★★★	★★★★	★★★	★★★	7
8	Dynaweb	★★★	★★★★	★★★	★★★★	★★★★	★★	★★★	8
9	Garden Gtunnel	★★★	★★★★	★★★★	★★★★	★★★★	★★	★★★	9
10	Your Freedom	★★★★	★★★★	★★★	★★★	★★★★	★★★	★★★	10
11	Freagate	★★★★	★★★★	★★★	★★★★	★★★	★★	★★★	11
12	JonDonym/ JAP	★★★★	★★★★	★★★	★★★	★★★	★★	★★★	12
13	Freenet				★★★	★★★★	★★	★★★	13
14	Hotspot shield	★★★	★★★	★★	★★★	★★★	★★	★★★	14

Once the results are combined with the in-country surveys, the ranking of some of the tools changes, causing tools that are more secure but slower to decline in ranking, such as Tor, which drops from position 3 to position 6.

Dynaweb

Developers

Dynaweb was launched in 2002 by Dynamic Internet Technology (DIT) with support of the U.S. government. The original aim of the tool was to provide access to internet sites banned in China. DIT clients include Voice of America, Human Rights in China (HRIC), and Radio Free Asia. DIT is a member of the Global Internet Freedom Consortium,²⁰ which is an alliance of organisations that develop anti-censorship technologies. Most of the alliance members have Chinese background, and are mainly affiliated with Falun Gong.

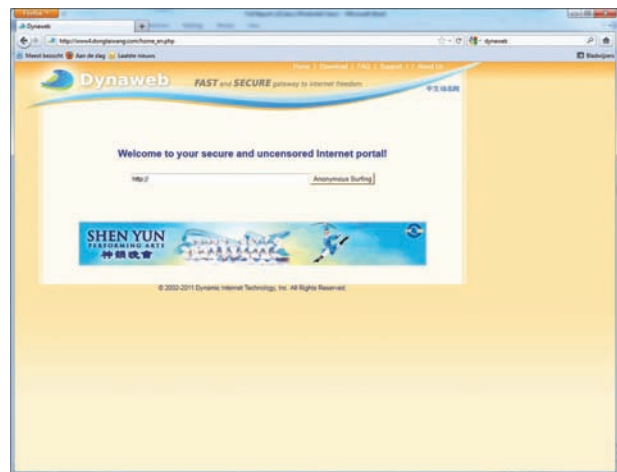
Since the 2009 uprising in Iran, Dynaweb has provided access to Iranian users. DIT's CEO, Bill Xia,²¹ is publicly known for his advocacy against the Chinese government. DIT's technology and its internal expertise are impossible to evaluate from an outsider's perspective. While DIT claims that their software constantly circumvents the Chinese Golden Shield Project, it offer no scientific or other evidence of this.

The history of DIT is a potential cause for concern. On several occasions, DIT's tools have been identified as a virus or a trojan by popular anti-virus products,²² and in early 2009, a web posting²³ about Dynaweb's potential use of personal data triggered an open discussion about the privacy policy of the project. Although none of these are sufficient to disqualify the tools involved completely, caution is appropriate when using them for particularly sensitive political activities online.



Tool: Dynaweb
Developers: Dynamic Internet Technology (DIT)
Website: www.dit-inc.us
Technology: Web proxy

	Survey	Test
Ease of Use:	★★★★	★★★
Performance:	★★★★	★★★★★
Security:	★★	★★★
Final Score:	★★★	



Technology

Dynaweb is a web-based proxy service. The tool uses a limited pool of proxy servers, most of them located in Taiwan.

Advantages

Due to the simplicity of the technology, the tool is very easy to use, as no special client software is needed. The developers focus their work in China. The Country surveys also saw a number of users commending the tool for its speed.

20 Global Internet Freedom Consortium
<http://www.internetfreedom.org/>
21 Bill Xia, a Chinese dissident (and Falun Gong practitioner) based in the US and is devoted to fight the Internet censorship of China.
22 Symantec re-labels Freegate http://www.theregister.co.uk/2004/09/16/symantec_relabels_freegate/ (last accessed
23 Freegate and Gpass sell user data, <http://blogs.law.harvard.edu/hroberts/2009/01/09/popular-chinese-filtering-circumvention-tools-dynaweb-freegate-gpass-and-firephoenix-sell-user-data/> (accessed 15-Feb-2011)

Disadvantages

The pool of proxy servers that Dynaweb is using are all equipped with uncertified SSL certificates that easily potentially be impersonated by a malevolent regime. This poses a security risk.

The URL that Dynaweb provides to users contains a fingerprint²⁴ that can be blocked by an application-layer firewall, such as in the following example:

**`http://us.dongtaiwang.com/do/Qa_k/
tttLwwwLx0LbC/`**

Confidentiality of the web requests is guaranteed by means of HTTPS, but unfortunately the SSL certificates used are not verifiable by a trusted root authority, making it feasible to impersonate the resources involved. Users of Dynaweb are easy to observe and can be linked to the technology by any monitoring agent who has access to internet traffic. Also, not all content is reachable via Dynaweb, as the proxy services decide what content falls under its service policy.

One of the most significant drawbacks of web-based proxies in general is their inability to properly translate flash and some other forms of dynamic content. For example, not many are able to open video websites, and perhaps may have some issues with complex social networking websites.

Being dedicated to users in China is also a disadvantage for users not living in China. The service's dedication to users in China is also a disadvantage for users outside of China.

24 All URLs contains the fingerprint "tttL"

Freagate

Developers

Freagate is another circumvention tool developed by DIT (See Dynaweb).

Technology

Freagate installs two local proxies with SOCKSv5 support in ports 8580 and 8567. The local proxy servers reach the external servers by means of HTTP, HTTPS, or SSL-based tunnel connections.

The external servers are mostly located in Taiwan (*.tfn.net.tw, *.hinet.net, *.seed.net.tw). Although Freagate seems to use several domain names around the world, the IP space is limited to a few providers located in Taiwan and the United States. No application-layer filters are provided that protect the user from Javascript, Java, or Flash identification attacks.

Although the company states that since January 2009 the tool is only available for Chinese and Iranian users, it was possible during the technical testing to bypass this geographic restriction.


Advantage

It is simple to use, as it is a downloadable client without and installer. It can be run as a portable application.

Disadvantage

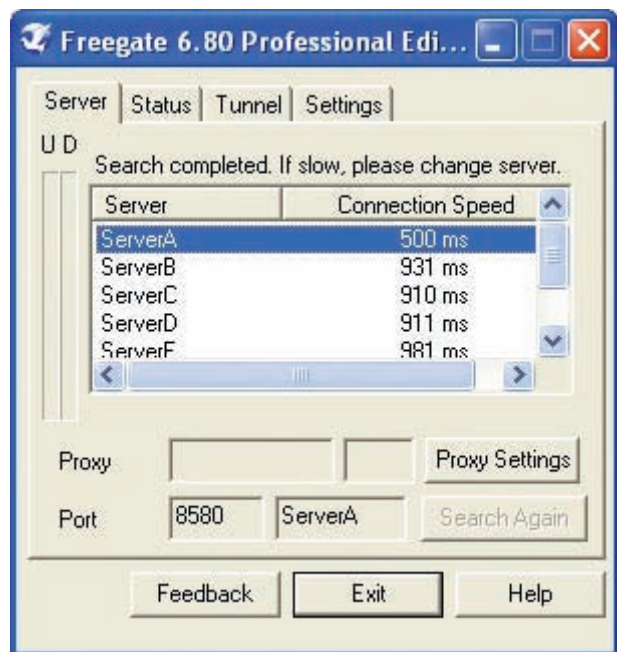
Just like Dynaweb, there is not much information available about the developers or the technology used. There are also many versions of the same software available, and it is not clear what differentiates one version from another.

The limited set of proxies is also a clear disadvantage.



Tool: Freagate
Developers: Dynamic Internet Technology (DIT)
Website: www.dit-inc.us
Technology: Local proxy (SOCKSv5)

	Survey	Test
Ease of Use:	★★★★	★★★★
Performance:	★★★	★★★★
Security:	★★	★★★
Final Score:	★★★	



GTunnel

Developers

Gtunnel was developed by Garden Networks for Information Freedom,²⁵ a nonprofit organization based in Canada. Since 2001, the organization had provided anti-censorship software to Chinese internet users.

Technology

GTunnel is a Microsoft Windows application that works as a local HTTP or SOCKS proxy server. Gtunnel modifies the proxy settings of Internet Explorer by modifying entries in the Windows registry and creates a local proxy on port 8081. As many other tools from the Global Internet Freedom Consortium, the proxy server, in turn, sets up HTTP and HTTPS connections (using destination ports 4443, 443, 80) to machines hosted in Taiwan (*.he.net).

One of the interesting aspects of Gtunnel is that it offers the possibility to channel the traffic through the Skype²⁶ or the Tor network. This makes the tool rank high in terms of availability. The software also claims that the traffic could be channelled through Gtalk but we were not able to verify this functionality.

One interesting aspect of the technology is the novel use of the Skype network as a transport layer, as this could provide better levels of anonymity and privacy while maintaining reliability.

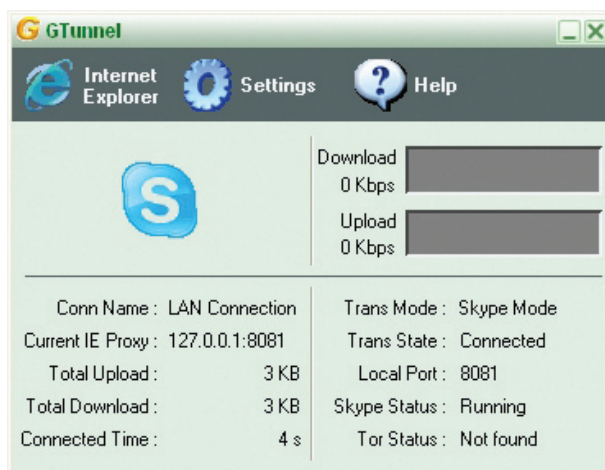
Advantage

The software includes a tunneling mechanism via the Skype network. By providing this mechanism, Gtunnel takes advantage of Skype's ability to build connections with other peers, even if this must be done through firewalls.

Garden Networks

Tool: Gtunnel
Developers: Garden Networks for Information Freedom
Website: www.gardennetworks.org
Technology: Local proxy (HTTP/SOCKS)

	Survey	Test
Ease of Use:	★★★★	★★★
Performance:	★★★★	★★★★
Security:	★★	★★★★
Final Score:	★★★	



Disadvantage

Gtunnel uses the same distributed network of proxies as Dynaweb and FreeGate. Although Gtunnel can use the Skype transport network to tunnel and hide their connections, our traffic analysis could identify traffic patterns of encrypted UDP traffic to Skype clients or super nodes in Taiwan. In countries where Skype is blocked, this functionality may be of limited use. The limited set of proxies is also a clear disadvantage.

²⁵ Website: www.gardennetworks.org.

²⁶ In our tests, we needed to use an old version of Skype (3.6).

Gpass

Developers

GPass was developed by the private company World's Gate Inc., another alliance member of the Global Internet Freedom Consortium. Little information can be found about the company or its developers, other than the CEO's name, Alex Wang.

The software was initially designed for China, but is also currently used in Iran.

Technology

Although GPass claims to be a different tool than Gtunnel, both tools seem to share the core technology. Gpass appears to be a re-branding of Gtunnel. GPass claims to be an integrated "anti-censorship software" that provides online security tools, encrypted storage, and personal data management tools in one single application. GPass is a downloadable client that must be installed on the users' computer.

Advantages

As one of the latest tools of the consortium, Gpass offers a very easy-to-use, free, and multi-featured tunnelling service with comprehensive documentation for the end user.

Disadvantage

The software has not been audited. As with any other circumvention tool based on a downloadable client, it can sometimes be challenging for the user to acquire the software, because the site distributing it is often blocked.



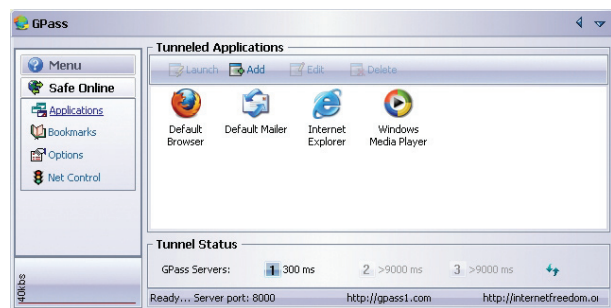
Tool: GPass
Developers: Word's Gate Inc
Website: <http://gpass1.com/gpass>
Technology: Multi-featured tunneling service

Survey

Test

Ease of Use:	★★★★	★★★★
Performance:	★★★★	★★★★
Security:	★★	★★★★★

Final Score: ★★★★★



Google (Reader, Translation, Cache)

Developers

Google Inc. is the company behind the Google search engine, Google Reader, and Google Translate. Although Google tools are not designed with circumvention properties in mind, Google's users have found creative ways to use their technology to reach blocked content.

Technologies

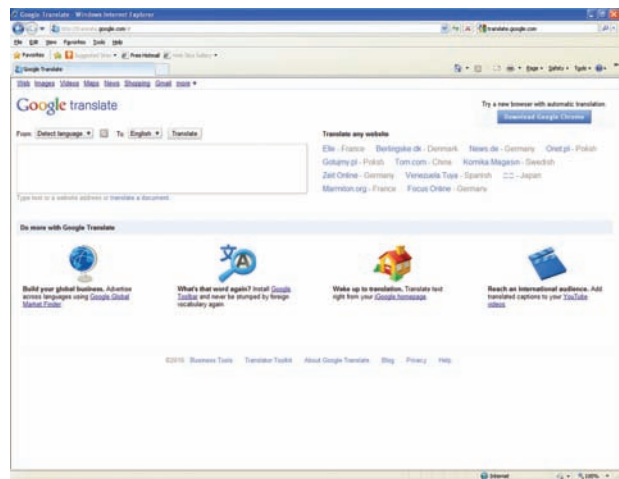
➤ **Google Cache:** A user can access Google's cache servers to gather blocked content. To find the pointer to the cached content, the user needs to reach the Google search engine first (so Google must not be blocked for this method to work). Some countries do block cache servers as well. It is known that Chinese firewalls can send reset (RST) packets to the queries containing the word "search?q=cache".²⁷ Using Google cache neither hides your IP nor the data being transferred (no HTTPS support), and so provides limited anonymity or communications privacy.

➤ **Google Reader:** Google offers users the possibility to subscribe to news feeds through Google Reader, which gathers data on the user behalf (it acts like a proxy), and lets the user read it through the Gmail web interface. From the outside, encrypted (HTTPS) traffic is sent between the user and Gmail. This solution requires that Gmail not be blocked. The user is limited to accessing content that is stored in RSS feed header. To read the full RSS entry, the user must be able to reach the source website directly.



Tool: Google
Developers: Google Inc.
Website: www.google.com
Technology: Website cache, translation

	Survey	Test
Ease of Use:	★★★★	★★★★
Performance:	★★★★	★★★★
Security:	★★★★	★★★
Final Score:	★★★★	



➤ **Google Translate:** Google's translation service can be used to gather blocked content. By setting the source language to something different from what it is, and setting the target language to the actual source language, Google Translate will gather the requested data and leave it non-translated. Google Translate does not provide HTTPS. As a result, web requests can be read in plain text on the wire.

27 <http://opennet.net/bulletins/006/>.

Advantage

The great advantage of Google's services are that they are widely adopted, and users all around the world are familiar with them. Additionally, no software is required for download, and all three "solutions" can be used on most public computers.

Disadvantage

These free services are not developed with anonymity and privacy in mind, and they therefore do not provide a secure service suitable for users in countries where heavy monitoring is taking place, or when they conduct particularly sensitive activities online.

These services cannot be used for websites that require user input, such as logins or the use of cookies (e.g, facebook).

Hotspot shield

Developers

Hotspot Shield is a software client developed by AnchorFree, which is a private U.S.-based company that was founded in early 2005 by David Gorodysky and Eugene Malobrodsky.

The purpose of the software is to put users in control of their internet activities, and to provide user privacy on the internet. The target audience is average internet users in democratic countries who seek secure connections while using insecure WiFi networks (such as for online shopping), not users in blocked countries.

The business model of this free software client relies on sponsored, personalized ads.

Technology

Hotspot Shield offers a VPN (virtual private network) between the client and the Hotspot Shield gateway. The software secures web sessions by HTTPS and thereby hides the user's IP address. The software is available for Windows and Mac OS. The software is available in .zip format, and needs to be unpacked and installed on a local machine. Once the software is launched, a browser is opened and directed to a local proxy (127.0.0.1). After a few seconds, the user is redirected to the site www.rss2search.com, an RSS feeds based search engine.

The search portal is full of ads, and gives the software a rather messy and unprofessional appearance. The user can either use one of the search engines provided (which are not easily identifiable), or can enter a correct URL into the browser address window. An attempt to visit Google.com, for instance results in a pop-up window with a cryptic question. If you answer incorrectly, the browser will redirect you to the default RSS search portal every time you try to access Google's search engine.

A web based (not RSS) search on "Burma election 2010" through Hotspot Shield (which uses the search-result.

com search engine) gives 187,000 hits²⁸ with a number of sponsored links presented on the top of the page. The sponsored links have very little to do with the actual search string entered; the first hit in this case is “Whistler 2010 Games” (the Olympic Winter Games).

Each page visited through Hotspot Shield is manipulated to include a banner that contains the Hotspot Shield logo and a commercial advertisement inserted in it. The advertisement can be removed from the web page by ticking a checkbox on every page visited, but the software logo remains.


Advantage

Hotspot Shield is a free VPN service that encrypts and then tunnels the traffic from the user to one of the Hotspot gateways. It is reported that their publicly known gateways remain unblocked in China.²⁹ Another advantage is that HotSpot tunnels all data regardless of the service. This is not the case with other forms of circumvention tools.

Disadvantage

Even after uninstalling the software, there are still Windows registry entries containing the string “Hotspot Shield” left on the computer.

AnchorFree allows third-party ad servers and ad networks to serve Hotspot Shield users with advertisements. The ads are sent directly to your browser, using the virtual IP address of the users machines assigned by Anchor Free. The ad servers are also free to use cookies, Javascript, and web beacons to measure the effectiveness of their advertisements and to personalize their advertising content. Personalized advertisements in an anonymizer-tool are not a recommended combination. It might work for a student circumventing a university block to access P2P networks, but is not recommended for a Burmese activist in Rangoon.



Tool:	Hotspot Shield	
Developers:	AnchorFree	
Website:	www.anchorfree.com	
Technology:	VPN	

	Survey	Test
Ease of Use:	★ ★ ★	★ ★ ★
Performance:	★ ★ ★	★ ★ ★
Security:	★ ★	★ ★
Final Score:	★ ★ ★	



Hotspot Shield - Mozilla Firefox

File Edit View History Bookmarks Tools Help

freedomhouse.org: Home Connecting...

http://127.0.0.1:895/config/?action=connect&lang=eng&afd=1302079417&...

Hotspot Shield
powered by AnchorFree

State: Connected

VPN IP Address: 10.51.40.29
VPN Server Address: x.x.x.0
Bytes In/Out: 9.04KB/4.43KB
Connected Since: 4/6/2011 10:43:49

[Disconnect](#)

[Details](#)

28 A Google search on the same string gives 2,550,000 hits.

29 How To Search Google Uncensored In China
<http://www.businessinsider.com/hotspot-lets-youcheck-google-in-china-2010-3>.

JAP

Developers

JAP is an open source Java based client program used to access the JonDonym anonymization service. JonDonym is a commercial spin-off from the AN.ON research project from the Dresden University of Technology (Germany) and the University of Regensburg (Germany) targeting "Protection of Privacy on the Internet."

Technology

JonDonym is a technology for anonymous proxy servers and is based on the principle of routing the traffic encrypted through several intermediaries (Mixes),³⁰ instead of using one single proxy server. Mixers are operated by external organisations, which are not a part of the project itself. Most of the mixers are hosted in Germany, but also in the Czech Republic, Denmark, the Netherlands, Switzerland, and the United States.

The technology not only provides anonymization of the user's identity and confidentiality (no one can read the content being sent), but it also ensures added privacy, since no single proxy server can identify the user and follow subsequent internet activities. In order to support many different applications, much like many other circumvention tools, JonDonym installs a local HTTP proxy (for web traffic), and a SOCKS proxy for applications such as email.

Advantage

JAP is available as a portable application (fully integrated with a number of PortableApps), which makes it an excellent client for internet care users. The trustworthiness of the software is very high due to the reputation of the developers (researchers from well respected universities), and the openness of the code (the source code is publicly available). The team behind

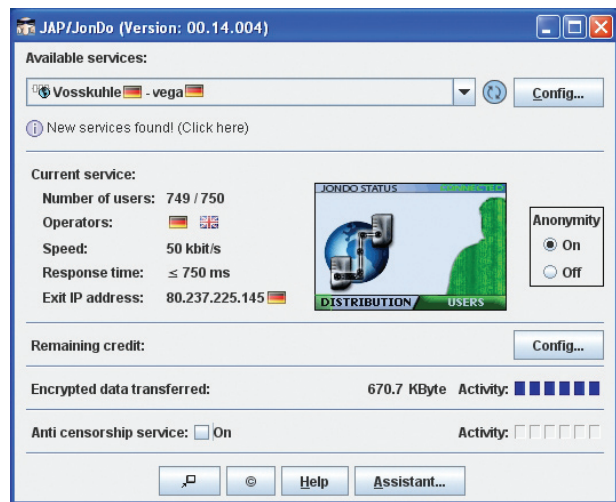
30 JAP uses an encryption technique known as telescopic encryption. The data is encrypted incrementally using the shared secrets of the exit node, intermediary and entry node. While the traffic travels in the chain, each of the intermediary "removes (peels-off: as in an onion)" one layer of encryption. This multi-layer encryption enables that every server involved in the chain only knows the next and previous hop of the data flow.



Tool: JAP
Developers: AN.ON research project, Dresden University of Technology (Germany), University of Regensburg (Germany)
Website: <http://anon.inf.tu-dresden.de>
Technology: Anonymous proxy server

	Survey	Test
Ease of Use:	★★★	★★★★
Performance:	★★★	★★★★
Security:	★★	★★★

Final Score: ★★★



the software is also open about theoretical threats³¹ to the software which the technology cannot provide protection against.

31 Assumption 1: A mix in the cascade should not be controlled by an attacker and should not work together with an attacker. Assumption 2: The attacker should not control all other users.

JAP offers the possibility of adding servers manually in case the central Info Server (the server aware of the status of the JAP network) is blocked.

The tool is also very flexible due to its support of both HTTP and SOCKS proxy. Furthermore JAP provides a Firefox bundle with existing open source tools to defend against common Javascript attacks.

Disadvantage

One disadvantage of JonDonym is that it is still a research project. In the past, JAP has been the target of police investigations, and the project is subject to the European legal requirement of data retention.³² Documentation³³ and localized GUI³⁴ are only available in English and German. The number of mixes and Mix Cascades are limited, and only 6 are available for free. This raises the issue of how well the technology compares, especially for non-premium (non-paying) users, and how easily the existing mixers can be blocked. As with Tor, the network has reportedly been slow.

32 Implementation of data retention according to the German Telecommunications Act -http://anon.inf.tu-dresden.de/dataretention_en.html.

33 Documentation is mainly available in English and German.

34 The installer and the GUI is localized to German, Czech, Dutch, French, and Russian.

Psiphon

Developers

Psiphon was initially developed by the CitizenLab at the University of Toronto. The group involved formed a commercial company, the SecDev Group, which continues to develop and support the product.

Psiphon was initially funded by the Open Society Institute. Since separating from the university in 2008, Psiphon has been established as a Canadian corporation and has received additional funding from a number of governments, mainly the United States and EU member states, including the United Kingdom.

Technology

Psiphon is a web proxy that uses the HTTPS protocol to transfer data securely between the user and the proxy server. It relies on a number of decentralized “in-proxies” that allow the user to connect to the central Psiphon proxy server via a number of different countries. The Psiphon architecture will then insert a “blue banner” into the browser window that can be used to surf the internet. The Psiphon server rewrites all the links and thus ensures that all traffic is relayed securely through its servers. Psiphon provides privacy, but not full anonymity, since the proxy server will log all client activity.

Another unique feature of Psiphon is that the solution relies on an invitation system. Users with a good history or trusted operators of in-proxies are allowed to invite new users to the system, making it harder for repressive governments to infiltrate and block the architecture.

Advantage

A great advantage of Psiphon is that the end user does not need to download and install any software. Hence, the use of Psiphon does not leave any trace on the users computer, as long as the browsing history is erased. This approach makes Psiphon an excellent solution for use in public internet cafes.

Documentation is available in five languages, and is comprehensive in terms of content, educational value, and illustrations.



Tool: Psiphon
Developers: Citizen Lab, Munk Centre for International Studies, University of Toronto, Canada.
Website: <http://psiphon.ca>
Technology: Web proxy (HTTPS)

Survey Test

Ease of Use:	★★★	★★★★★
Performance:	★★★★★	★★★★★
Security:	★★★	★★★★★
Final Score:	★★★★★	



Disadvantage

Although the “trust model” is a useful solution to the problem of untrusted public proxy servers, it can also serve as a bottleneck, as not everyone in a blocked country knows someone that can provide access to a Psiphon node. Hence, the accessibility of Psiphon is presumably lower compared to other proxy servers that are open to the public. As with other web-based proxies, the service may be less suitable for flash-based video content or complicated dynamic content, although the Psiphon team is reportedly able to occasionally adapt their service to such content. Logging practices (Psiphon stores all events on its services) have also been reported as a potential downside of this product. This was not verified in the technical testing. Also, the service appears to use self-signed certificates, which makes man-in-the-middle attacks easier.

Tor

Developers

The Tor Project is a nonprofit organisation based in the United States. Tor is the latest implementation of an onion routing system. Tor started as a continuation of the onion routing research project originally funded by the Office of Naval Research (ONR) and DARPA. Tor or “the second generation onion routing protocol” was officially presented in 2004 by Roger Dingledine, Nick Mathewson, and Paul Syverson.

Although Tor was originally designed to protect government communications, the project has extended its target group to a diverse group of users that includes the military, journalists, law enforcement officers, and activists. Tor currently receives funding from governments, NGOs, and individuals. Tor has managed to assemble a large community of users and developers that benefit from its publicly available source code and protocol specification.

Technology

The Tor project’s main goal is to develop a network that protects the privacy of TCP connections. Tor’s basic principle is to route internet traffic around a distributed network of relays run by volunteers. Tor uses an encryption technique known as onion routing, or telescopic encryption. The data is encrypted incrementally using the private key of the exit node, intermediary, and entry node.

Tor was not originally designed as a circumvention tool, but rather as a mechanism to resist traffic analysis attacks. Since Tor channels the traffic via a virtual circuit, it enables the user to circumvent internet blocking. The common method to block Tor is to restrict access to the seven directory (authoritative) servers that offer a directory of the nodes in the network.³⁵ To strengthen the resistance against this kind of attack, Tor developers

35 Blocking Tor servers <http://blog.vorant.com/2008/06/tor-server-lists-revisited.html>.



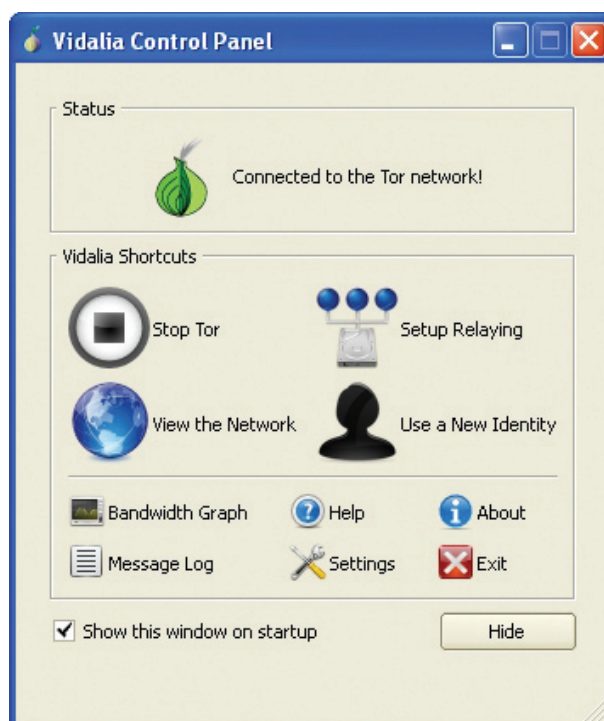
Tool: Tor
Developers: Tor Project, a US based non-profit.
Website: www.torproject.org
Technology: onion routing/telescopic encryption

Survey

Test

Ease of Use: ★★★ ★★★★★
Performance: ★★★★★ ★★★★★
Security: ★★ ★★★★★

Final Score: ★★★★★



have extend their protocol to encrypt directory lookups, and now allow users to use intermediaries not published in the directory to relay the traffic to them. These new

intermediaries are known as “Tor bridges” and their IP addresses can be retrieved by alternatives means (mail requests, internet messaging, etc.).³⁶

Additionally, the Tor project aims to provide basic application-level anonymity by including a proxy that filters personal data in web requests from a Firefox web browser.

One highlight of Tor is that the technology allows clients and relays to offer hidden services. Hidden services are internet services that can be offered inside of the Tor network without revealing the IP address to its users.

Advantage

Tor is one of the most technically advanced projects in the area of resisting traffic analysis. Their website clearly describes what the tool can and cannot do. Their infrastructure is highly distributed, with the bundle of tools in one single installer (below is the screenshot of the Vidalia control panel, which runs on many different platforms), making the technology accessible to average users.

Disadvantage

Tor’s developers are aware of a number of limitations of Tor.³⁷ The overall perception is that the Tor network is slow.³⁸ Tor does not behave well in highly congested internet connections, and although efforts are documented to improve Tor’s behaviour,³⁹ non-technical users will struggle to fine-tune the software.

Although there are some efforts to facilitate the deployment of Tor in the form of distributions (e.g., Incognito, tor ramdisk, open-dd wrt), they seem to be insufficient to convince average users to trade their connection speed for the added security and privacy that Tor offers.

36 Tor partially blocked in China <https://blog.torproject.org/blog/tor-partially-blocked-china>.

37 Why tor is slow? <https://blog.torproject.org/blog/why-tor-is-slow>.

38 Performance is measured also by the Tor Metrics Portal, see <https://metrics.torproject.org/performance.html>. The metrics portal holds per country data on usage at <https://metrics.torproject.org/users.html>, which can be interesting to watch in times of crisis.

39 Improving Tor speed <https://trac.torproject.org/projects/tor/wiki/TheOnionRouter/FireFoxTorPerf>.

Ultrasurf

Developers

Ultrasurf is another product from the Global Internet Freedom Consortium, developed by UltraReach, a group of entrepreneurs based in the United States, but with roots in China. The team of developers behind the tool is not public, and very little information about UltraReach is available on their website. The main focus of Ultrasurf is providing circumvention for Chinese internet users.

Technology

UltraSurf uses HTTP proxy servers to allow users to access blocked content. Limited technical details are available on the website, which only mentions a little-known technology called GIFT (Global Internet Freedom Technology) which happens to be the same technology that the UltraReach team developed. The technology is neither openly documented nor described.

The software provides a quick and easy way for blocked users to access web content through their preferred browser (Internet Explorer or Firefox).

Advantage

Ultrasurf is free, small in size, easy to hide in a computer, and discrete during usage. The performance is excellent, and it does not require any installation. Ultrasurf does not change any Windows registry entries (neither during installation nor usage), and can be uninstalled by simply deleting the executable file.

Disadvantage

During the last couple of years, there have been accusations on internet forums that Ultrasurf contains Trojans and viruses. Although unusual behaviour has been documented on computers that have Ultrasurf installed, there has not been a clear and proven case against the tool. Ultrasurf has simply denied that this problem exists. The UltraSurf website, states that "UltraSurf provides users with state-of-the-art internet technology to break through firewall safely. It is popular anti-censorship software, not a Trojan or virus. Please rest assured that UltraSurf will not touch any of the documents on your PC."



Tool: UltraSurf
Developers: UltraReach
Website: <http://www.ultrareach.com>
Technology: HTTP proxy

	Survey	Test
Ease of Use:	★★★★	★★★★
Performance:	★★★★	★★★★
Security:	★★★	★★★★
Final Score:	★★★★	



Otherwise, little is known about the infrastructure used to provide the service. It appears to use an encrypted tunnel to the Ultrasurf infrastructure to bypass any blockades, although little evidence is present to support this.

Your Freedom

Developers

Your Freedom was developed by the German company Reichert Network Solutions (re:solution), which is run by Christian Reichert. A basic service is offered for free, while a number of premium levels can be purchased based on a voucher system. The free version of this software is restricted in terms of bandwidth and number of simultaneous streams.

Technology

Your Freedom is a proxy tunnelling solution (HTTP and SOCKS) with support for HTTPS, FTP and UDP services. The software allows web browsers, chat services and file sharing applications to access the central network of proxy servers.⁴⁰ The software is Java based, and is available for Windows, Linux and Mac OS.

The developer highlights that Your Freedom is not a perfect anonymizer, since the software cannot protect the end user from end user mistakes or pre-existing flaws in applications and protocols (which could reveal the user's IP address). Your Freedom hides the user's IP address unless an application being used carries it "inband" (for example in HTTP headers or flash applications).

Advantage

The software is simple to use although it provides privacy and anonymity with sophisticated methods. The extensive instruction manual provides an excellent resource to learn about the tool and understand its underlying technology. The guide explains what protection the tool provides and does not provide. It explains which information is logged by the proxy servers, and for what use. Furthermore, the developer provides a GPG key for contact regarding sensitive issues. Your Freedom offers a mechanism known as CGI Relays⁴¹ to support the limited number of proxy servers.

40 The network consists of 18 proxies located in 3 countries.

41 CGI Relays <http://www.your-freedom.net/index.php?id=156>.



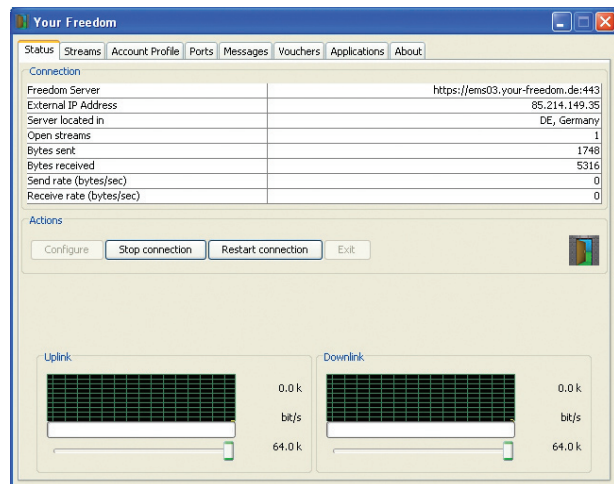
Tool: Your Freedom
Developers: re:solution - Reichert Network Solutions, Germany
Website: www.your-freedom.net
Technology: Proxy tunnelling software (HTTP/SOCKS) with support for HTTPS, FTP and UDP services.

Survey

Test

Ease of Use:	★★★★	★★★★
Performance:	★★★★	★★★★
Security:	★★★	★★★

Final Score: ★★★★★



Disadvantage

The primary target group for the tool is average internet users who are restricted by a firewall (such as at school or work). The tool is designed to circumvent blocking, with little focus, however, on hiding the existence of the tool,⁴² or providing a clean un-installation,⁴³ portability,⁴⁴ or easy access to the tool.⁴⁵

42 The tool needs to be locally installed on the computer.

43 Using the un-install feature leaves several Windows registry entries containing the name "Your Freedom"

44 The tool cannot be run portable.

45 The user needs to register online, activate her account (by email invitation), to download the software.

In-Country Survey Results



In-Country Survey Results

The table below describes the main findings of the general questions section of the user survey for each country.⁴⁶

	Azerbaijan	Burma	China	Iran
Access method	Internet cafe	Internet cafe	Home PC	Home PC
Speed	Dial-up	Dial-up	Broadband	Broadband
Blocked Content	Low	Medium	Low	High
Access	Website	Website	Website	Website
Most important	Ease of use	Security	Speed	Speed
User Level	Medium	Medium	Medium	Medium
Winning tool	Google	Google	Freenet	VPN

A key differentiator among the user surveys in the countries under review is the method of internet access. The more affluent societies, such as China and Iran, consider home computers as a predominant access method, whereas the predominant access method in Azerbaijan and Burma is through internet cafes.

The survey of tools for each country produced remarkable differences with the laboratory tests, mostly in terms of perceived security. Whereas the laboratory tests highlighted the lack of security when using tools such as Google (where it is unlikely that specific design-criteria included censorship or circumvention-related requirements), users still perceived these tools to be secure, and were well supported.

The procedures used to block content on the internet varies widely. The complexity of state blocking systems increases dramatically based on the selection of content types to be blocked; the desired effectiveness and efficiency of the blocking systems; and the specific concerns of the government.

⁴⁶ This overview is based on the majority of the answers received per country – even if percentages for a second choice are not far apart.

**Table: Summarized results from all countries,
scored by subjective user experiences**

Overall Country Surveys		Ease of Use	Performance	Support & Security	Overall
1	Dynaweb	★★★★	★★★★	★★	★★★
2	Freegate	★★★★	★★★	★★	★★★
3	Freenet	★★★	★★★★	★★	★★★
4	Garden GTunnel	★★★★	★★★★	★★	★★★
5	Google (Translate Reader Cache etc.)	★★★★	★★★★	★★★★	★★★★
6	GPass	★★★★	★★★★	★★	★★★
7	Hotspot Shield	★★★	★★★	★★	★★★
8	JAP	★★★	★★★	★★	★★★
9	Proxy	★★★★	★★★★	★★★	★★★
10	Psiphon	★★★★	★★★★	★★★	★★★★
11	Tor	★★★	★★★★	★★	★★★
12	Ultra Surf	★★★★	★★★★	★★★	★★★★
13	Your Freedom	★★★★	★★★★	★★★	★★★★
14	VPN	★★★	★★★★	★★★	★★★

Note: The score for each tool is determined by averaging the scores for all three categories (which are in turn calculated from a range of items as outlined in the methodology). The stars are allocated based on these scores; even where tools show the same number of stars, the final detailed score is often different creating a specific tool ranking.

Table: Country comparison of all tools, scored by subjective user experiences

Country Comparison		Azerbaijan	Burma	China	Iran
1	Dynaweb	★★★	★★★★	★★★★	★★★
2	Freerate	★★★	★★★	★★★★	★★★
3	Freenet	★★★	★★★	★★★★★	★★★
4	Garden GTunnel	★★★★	★★★	★★★	★★★
5	Google (Translate Reader Cache etc.)	★★★★	★★★★	★★★★	★★★★
6	GPass	★★★★	★★★★	★★★	★★★
7	Hotspot Shield	★★★	★★★	★★★	★★★
8	JAP	★★★	★★★	★★★★	★★★
9	Proxy	★★★★	★★★★	★★★	★★★
10	Psiphon	★★★★	★★★★	★★★	★★★
11	Tor	★★★	★★★	★★★	★★★
12	Ultra Surf	★★★★	★★★★	★★★★	★★★
13	Your Freedom	★★★★	★★★★	★★★★	★★★
14	VPN	★★★	★★★	★★★★	★★★★

Importance of Speed Versus Security

A surprising result from the in-country surveys is that the users generally indicated a preference for speed of operation over security and anonymity of the communication. This may be explained by faltering or absent enforcement towards the majority of users who wish to receive blocked content, whereas only a minority of users employ circumvention tools to transmit politically sensitive communication. This specific issue was not addressed further in the survey, however.

Aspects of Circumvention Tools User Preferences	
Speed of Operation	★★★★
Security and Anonymity	★★★
Ease of Use	★★
Support Services	★
Other	★

Acquiring tools

Another interesting finding, perhaps especially for tool developers, is that the majority of users appeared to receive their circumvention tools through websites. Only in Burma was the distribution also largely reliant upon hand-delivery of the tools through physical media.

How do you acquire the majority of the tools you use?	Iran	Azerbaijan	Burma	China	Total
Website	★★★★	★★★★★	★★	★★★★★	★★★★★
Email	★	★	★★	-	★
USB/DVD/CD	★	-	★	-	★
Other – please specify	★	-	-	-	-

Republic of Azerbaijan

Public sources of the blocking employed and the government's attitude towards free speech online

There is some evidence of censorship, although the methods employed do not seem comprehensive or pervasive. A number of journalists who have criticized government officials in the course of their work have been subject to harassment, threats, and acts of physical violence that appeared to be connected to their criticism of the government or public officials. Reporters Without Borders reported that independent and opposition journalists have been under constant pressure because of their work.⁴⁷ Anecdotal evidence of the regime's restrictive attitude towards free speech includes the 2009 arrest of pro-democracy bloggers.⁴⁸

In Azerbaijan, for instance, defamation can carry as long as a two-year prison sentence, and insulting someone can carry a six-month prison sentence.⁴⁹

It is widely believed that the Ministry of National Security and the Ministry of Internal Affairs monitor telephone and internet communications, particularly those of foreigners, prominent political and business figures, and individuals engaged in international communication. In one such incident, the Ministry of National Security identified and questioned many of the 43 people who voted via text message for the Armenian entry into the annual Eurovision song contest.⁵⁰

According to the U.S. State Department in their annual 2009 Human Rights Report, there was no evidence to confirm the widely-held belief that the government monitored the internet activities of foreign businesses or opposition leaders. During 2009, authorities temporarily blocked access to a web site supporting jailed youth

Quick facts Azerbaijan

Land Area:	86,600 sq km *
Population:	8,997,400 (Jan 2010)
Urban population:	54% of total population (2010)
Religions:	Muslim 93.4% Russian Orthodox 2.5%, Armenian Orthodox 2.3%
GDP per capita:	\$9,953 (IMF Estimate)
Telephones fixed:	1.397 million (2009)
Telephones gsm:	7.757 million (2009)
Internet hosts:	22,737 (2010)
Internet users:	2.42 million (2009)
Natural resources:	Petroleum, natural gas, iron ore, nonferrous metals, bauxite

* Includes the exclave of Naxcivan Autonomous Republic and the Nagorno-Karabakh region; the region's autonomy was abolished by Azerbaijani Supreme Soviet on 26 November 1991.



activists Emin Milli and Adnan Hajizade. Authorities also blocked public access to two web sites of an independent nonprofit, the Election Monitoring Center, although the sites were accessible from abroad.⁵¹

According to a 2010 report endorsed by Freedom House, the online media fill an important gap in coverage of

47 Idem - <http://www.state.gov/g/drl/rls/hrrpt/2009/eur/136020.htm>.

48 <http://gigaom.com/video/censorship-fail-azerbaijan-jails-video-bloggers-for-donkey-video/>

49 <http://www.osce.org/files/documents/b/b/13836.pdf>.

50 Idem - <http://www.state.gov/g/drl/rls/hrrpt/2009/eur/136020.htm>.

51 Idem - <http://www.state.gov/g/drl/rls/hrrpt/2009/eur/136020.htm>.

current events, although they are under increasing pressure due to censorship.⁵²

According to the OpenNet Initiative, the internet in Azerbaijan remains largely free from direct censorship despite the government's heavy-handed approach to political opposition and evidence of second- and third-generation controls.⁵³

Survey Results

In accordance with these findings, the user survey for Azerbaijan displayed a relatively low incidence of blocked content.

Google was the leading utility for most of the questions, and is the logical choice given slow internet speeds and preferences for usability. Google was ranked first for all three categories.

It would appear, also, that the internet user community has so far relied on internet cafes to provide the required anonymity. For politically sensitive speech, adding more secure circumvention methods would be advisable.

VPN technology was not well-liked, probably due to the need to have end-point relationships in order to establish an international VPN. This should be considered as a service offered by internet ISP's in democratic countries.

Your Freedom was ranked as second in the Ease of Use and Performance categories, but Psiphon was ranked second in the Support and Security category.

Table: Results from Azerbaijan, scored by subjective user experiences

Results for Azerbaijan		Ease of Use	Performance	Support & Security	Overall
1	Dynaweb	★★★★	★★★★	★★	★★★
2	Freegate	★★★★	★★★★★	★★	★★★
3	Freenet	★★★★	★★★★	★★	★★★
4	Garden GTunnel	★★★★	★★★★	★★	★★★★
5	Google (Translate Reader Cache etc.)	★★★★★	★★★★★	★★★★	★★★★★
6	GPass	★★★★	★★★★	★★★	★★★★
7	Hotspot Shield	★★★★	★★★★	★★	★★★
8	JAP	★★★	★★★★	★★	★★★
9	Proxy	★★★★	★★★★★	★★★	★★★★★
10	Psiphon	★★★★	★★★★	★★★★★	★★★★★
11	Tor	★★★	★★★★	★★	★★★
12	Ultra Surf	★★★★	★★★★★	★★★	★★★★★
13	Your Freedom	★★★★	★★★★★	★★★	★★★★★
14	VPN	★★★	★★★★	★★	★★★

52 <http://www.indexoncensorship.org/wp-content/uploads/2010/10/free-expression-under-attack.pdf>.

53 <http://opennet.net/research/profiles/azerbaijan> (last accessed 16-feb-11)

Burma

Public sources of the blocking employed and the government's attitudes towards free speech online

The U.S. State Department's 2009 Human Rights Report indicates that internet access and usage is extremely limited, due to government restrictions and lack of infrastructure. According to the International Telecommunication Union, in 2008 the number of internet subscribers was less 0.04 percent of the population, and only 0.2 percent of inhabitants used the internet, mostly in urban internet cafes. Authorities frequently blocked access to web sites attracting many users or large attachments related to political issues. Email messages sometimes took several days to arrive in a receiver's inbox, often with attachments deleted. While the government rarely charged people explicitly for expressing political, religious, or dissenting views in electronic forums, including email, it often charged those suspected of such activities with other crimes. Nay Phone Latt (Nay Myo Kyaw), internet blogger and owner of three internet cafes, who in November 2008 was sentenced to over 20 years in prison, remained detained at year's end.⁵⁴

Stringent control and regulated access is omnipresent according to the OpenNet Initiative and several independent websites.⁵⁵ In 2007, the government disconnected the entire country during politically-motivated unrest.

A country study by the Berkman Center for Internet and Society, funded by the OpenNet Initiative, indicated that internet access is costly, and that the state uses software-based filtering techniques to severely limit the materials that Burmese can access online. Most dial-up internet accounts provide access only to the limited Myanmar Internet, not to the global network that most people

Quick facts Burma

Land Area:	676,578 sq km
Population:	53,414,374
Urban population:	33% of total population (2008)
Religions:	Buddhist 89% Christian 4% Muslim 4%
Telephones fixed:	812,000 (2009)
Telephones gsm:	448,000 (2009)
Internet hosts:	172 (2010)
Internet users:	110,000 (2009)
Natural resources:	petroleum, timber, tin, antimony, zinc, copper, tungsten, lead, coal, marble, limestone, precious stones, natural gas, hydropower.



around the world can access. The state maintains the capability to conduct surveillance of communication methods such as email, and to block users from viewing web sites of political opposition groups, organizations working for democratic change in Burma, and pornographic material.⁵⁶

54 <http://www.state.gov/g/drl/rls/hrrpt/2009/eap/135987.htm>

55 http://en.wikipedia.org/wiki/Censorship_in_Burma ; <http://opennet.net/blog/2008/10/burma-steps-up-internet-restrictions>; <http://opennet.net/research/profiles/burma> (all last accessed 14-Feb-11);

56 http://cyber.law.harvard.edu/publications/2005/Internet_Filtering_in_Burma_in_2005 (last accessed 7-Mar-2011)

Survey Results

Google services are the top choice for Ease of Use in Burma and second for Support and Security. UltraSurf scored highest for Performance, and Psiphon for Support and Security.

A higher incidence of blocked content and a stringent regime on free speech no doubt explain the almost equal appreciation of Ease of Use, Performance, and Security. Most information on the tools is learned from colleagues and friends.

The users completing the survey indicated an even mix of beginner, intermediate, and advanced skill levels, with over half of users using circumvention tools often or always.

It is interesting to note that the test winner for Burma does not provide a high level of security. This is likely a result of the primary use of internet cafes (with the second choice being work computers) as the preferred method of access to the Internet. The reason is that installing circumvention tools in either of these environments is rarely easy, so a web-based proxy system seems an obvious way to circumvent such restrictions.

Table: Results from Burma, scored by subjective user experiences

Results for Burma		Ease of Use	Performance	Support & Security	Overall
1	Dynaweb	★★★★	★★★★	★★	★★★★
2	Freerate	★★★★	★★★★	★★	★★★
3	Freenet	★★★★	★★★★	★★	★★★
4	Garden GTunnel	★★★★	★★★★	★★	★★★
5	Google (Translate Reader Cache etc.)	★★★★★	★★★★	★★★★	★★★★
6	GPass	★★★★	★★★★	★★★	★★★★
7	Hotspot Shield	★★★★	★★★	★	★★★
8	JAP	★★★	★★★	★	★★★
9	Proxy	★★★★	★★★★	★★★	★★★★
10	Psiphon	★★★★	★★★★	★★★★	★★★★
11	Tor	★★★	★★★	★★	★★★
12	Ultra Surf	★★★★	★★★★	★★★	★★★★
13	Your Freedom	★★★★★	★★★★	★★★	★★★★
14	VPN	★★★	★★★	★★	★★★

China

Public sources of the blocking employed and the government's attitude towards free speech online

China has a highly extensive filtering scheme for political and national security reasons. It is based on content scanning (key word searching in HTTP traffic). According to the International Center for Human Rights and Democratic Development, "China's Golden Shield project threatens the protection of human rights, in particular the right to privacy—a right that underpins other essential elements of democracy activism such as freedom of association and freedom of expression."⁵⁷ The OpenNet Initiative agrees that "China has devoted extensive resources to building one of the largest and most sophisticated filtering systems in the world. The golden shield or "Great firewall" that stops communications to unwanted content has a few flaws, however."⁵⁸

Survey Results

China has a well-developed internet infrastructure with a somewhat more liberal regime towards mass internet access. This might be due to the difficulty of managing the online activities of such a large population.

Comprehensive filtering is present, though according to the survey results, does not disrupt users too greatly. However, it should be noted that the users who completed the in-country survey are likely to be using circumvention tools already. Those who know how to use circumvention tools such as Freenet are not restricted in terms of access. Yet, there are many less tech-savvy internet users in the country whose internet access is restricted by the filtering system.

Quick facts China

Land Area:	9,596,961 sq km
Population:	1,330,141,295 (July 2010 est.)
Urban population:	43% of total population (2008)
Religions:	Daoist (Taoist), Buddhist Christian 3%-4%, Muslim 1%-2% officially
Telephones fixed:	313.68 million (2009)
Telephones gsm:	747 million (2009)
Internet hosts:	15.251 million (2010)
Internet users:	389 million (2009)
Natural resources:	Coal, iron ore, petroleum, natural gas, mercury, tin, tungsten, antimony, manganese, molybdenum, vanadium, magnetite, aluminum, lead, zinc, rare earth elements, uranium, hydropower potential (world's largest).



Proxy-based solutions (Freenet won the user survey) seem a logical test winner, but special care is needed for politically sensitive communications, as repression of political speech is very common and frequently leads to imprisonment.

57 http://www.dd-rd.ca/site/_PDF/publications/globalization/CGS_ENG.PDF.

58 <http://opennet.net/research/profiles/china>.

Table: Results from China, scored by subjective user experiences

Results for China		Ease of Use	Performance	Support & Security	Overall
1	Dynaweb	★★★★	★★★★	★★★★	★★★★
2	Freegate	★★★★	★★★★	★★★	★★★★
3	Freenet	★★★★★	★★★★★	★★★★	★★★★★
4	Garden GTunnel	★★★	★★★	★★★	★★★
5	Google (Translate Reader Cache etc.)	★★★★	★★★★	★★★★	★★★★
6	GPass	★★★★	★★★	★★★	★★★
7	Hotspot Shield	★★★★	★★★	★★★	★★★
8	JAP	★★★★	★★★★	★★★	★★★★
9	Proxy	★★★★	★★★★	★★★	★★★
10	Psiphon	★★★★	★★★	★★★	★★★
11	Tor	★★★★	★★★	★★★	★★★
12	Ultra Surf	★★★★	★★★★	★★★	★★★★
13	Your Freedom	★★★★	★★★	★★★	★★★★
14	VPN	★★★★	★★★★	★★★	★★★★

Iran

Public Sources of the blocking employed and the government's attitude towards free speech online

The 2007 Human Rights Report from the United Kingdom's Foreign and Commonwealth Office reported that Iran continues to deny its people the right to express their opinions freely and peacefully, and restrictions have increased over the last 18 months. Journalists and editors have been arrested for printing articles deemed to be offensive or un-Islamic. The report confirmed that the internet continues to be a target of government restrictions, with access to many websites and blogs (which often provide news and critical commentary) blocked. In early 2007, internet connection speeds were slowed down, probably to restrict access to foreign websites and audiovisual internet services, and an attempt was made to get all website managers and bloggers to register their websites with a government agency.⁵⁹

Censorship in Iran is invasive, and according to most respondents, blocking occurs during every internet session. According to some public sources, most content is vetted before being made accessible, displaying the pervasive nature of Iran's censorship practises.

As of 2006, Iran's censorship software is configured to filter local Persian-language sites, and block prominent English-language sites, such as the websites for the New York Times, Amazon.com, IMDB.com, and Facebook.

The U.S. State Department reported that in 2009, the government monitored internet communications, especially via social networking websites such as Facebook, Twitter, and YouTube, with technology it purchased at the end of 2008. The government threatened, harassed, and arrested individuals who posted comments critical of the government on the

Quick facts Iran

Land Area:	1,648,195 sq km
Population:	76,923,300 (July 2010 est.)
Urban population:	68% of total population (2008)
Religions:	Muslim 98% (Shia 89%, Sunni 9%), other (includes Zoroastrian, Jewish, Christian, and Baha'i) 2%
GDP per capita:	\$5,247 (2008)
Telephones fixed:	25.804 million (2009)
Telephones gsm:	52.555 million (2009)
Internet hosts:	119,947 (2010)
Internet users:	8.214 million (2009)
Natural resources:	Petroleum, natural gas, coal, chromium, copper, iron ore, lead, manganese, zinc, sulfur hydropower potential (world's largest).



internet; in some cases it reportedly confiscated their passports or arrested their family members.⁶⁰

According to Wikipedia, the technical solution that enables the blocking appears to be based on U.S. technology.⁶¹ An OpenNet Initiative Report published

59 United Kingdom Foreign & Commonwealth Office Human Rights Annual report 2007 available at <http://www.fco.gov.uk/resources/en/pdf/human-rights-report-2007>.

60 US State Department - 2009 Country Reports on Human Rights Practices, available on <http://www.state.gov/g/drl/rls/hrrpt/2009/nea/136068.htm>.

61 See http://en.wikipedia.org/wiki/Censorship_in_Iran; <http://>

in June 2009 reported that “a centralized system for internet filtering has been implemented that augments the filtering conducted at the Internet service provider (ISP) level. Iran now employs domestically produced technology for identifying and blocking objectionable websites, reducing its reliance on Western filtering technologies.”⁶²

Survey Results

With most internet access taking place from home PCs, the obvious choice here is a generic tool (VPN) that circumvents the very stringent blocking system. VPN is widely used by large corporation for staff who work outside the office for long periods of time, and provides secure access to company servers.

It also permits all network communications to be routed from a remote site to, and through, the central network connection and bypass all local networking problems and blocks. For individual users, whereas a VPN provides a high level of circumvention, VPN can sometimes be difficult to setup and does require a remote connection point outside the area of blocking to receive the connection. Google services are a popular choice, since Google uses standard software solutions (secure website connections). Use of Google services does not require any special software to be installed (apart from a web browser), and is therefore easier from a blocked area, unless access to Google itself is blocked.

Table: Results from Iran, scored by subjective user experiences

Results for Iran		Ease of Use	Performance	Support & Security	Overall
1	Dynaweb	★★★	★★★	★★	★★★
2	Freegate	★★★★	★★★	★★	★★★
3	Freenet	★★★	★★★	★★	★★★
4	Garden GTunnel	★★★	★★★	★★	★★★
5	Google (Translate Reader Cache etc.)	★★★★	★★★★	★★★★	★★★★
6	GPass	★★★	★★★	★★	★★★
7	Hotspot Shield	★★★	★★★	★★	★★★
8	JAP	★★★	★★★	★★	★★★
9	Proxy	★★★	★★★	★★	★★★
10	Psiphon	★★★	★★★	★★	★★★
11	Tor	★★★	★★★	★★★	★★★
12	Ultra Surf	★★★★	★★★	★★★	★★★
13	Your Freedom	★★★	★★★★	★★★	★★★
14	VPN	★★★★	★★★★	★★★★	★★★★

opennet.net/studies/iran#toc2d;
<http://opennet.net/research/profiles/iran/>.

62 <http://opennet.net/research/profiles/iran/>.

Findings and Recommendations



Findings and Recommendations

Findings

This report shows that the many tools available for circumventing state-sponsored blocking perform reasonably well in terms of ease-of-use, performance, and security when technical laboratory testing is conducted. Although differences do exist, the primary finding of this report is that differences are marginal and most tools perform well. Differences may be observed in the ratings displayed in the extensive tools section. Each user must select a tool and a strategy for their needs and environment. Not every tool is equally suited for every user. This is due to differences in the censorship and blocking methods involved, and also due to the internet access methods (and locations) involved in the countries that were investigated. Where lower speeds and internet cafes are predominant, there is a limited choice of tools available, especially where installing or running software on a public computer is made impossible.

An important factor is the nature of the user's communication. Those merely accessing moderately-sensitive content might forego advanced security and encryption, in essence trading speed for security, and may well be less concerned about the traces the software leaves on their computer. Keen political activists should, however, not compromise on the security of communications, choosing often slower, more secure tools. They will also need to be concerned about the traces a tool leaves on their computer. Home users, and especially those with higher access speeds, will benefit from more advanced tools, while others, who are limited to a dial-up connection under heavy censorship, may find that only a few tools, sometimes even with limited security, are useable in their situation.

Overall, users seem to require a high speed of operation when it comes to selecting a tool. Delays involved in onion routing seem to make this highly secure architecture less attractive for this reason. A slow connection, combined with the often lower speed of

telescopic-crypto based solutions, may make internet access impossible in countries that are limited to dial-up access. Paid subscriptions may be needed there, although, in the countries investigated, these will present risks and problems in their own right. Payment, for instance, may not be easy and is harder to do anonymously.

A major finding is that tools used for circumvention are not necessarily suitable for privacy protection. Some do not even hide the contents of the communication. Even if such a tool is used, the origin of the encrypted content can never be fully hidden from a regime if it has control over the transmission infrastructure. There appears to be little awareness about the risks involved in using such technologies, which can be easily spotted by those who monitor the networks.

This is especially worrying, again, for users that transmit politically sensitive speech, since they will often be targeted with technical and non-technical methods alike by the regimes that perform censorship on such an extensive scale. Whereas the average user of a circumvention tool may merely be flagged by a regime for displaying unwanted political interest, those actively disseminating critical political speech should certainly take special care to hide the content of their communication and take care to cover their tracks. Not doing so may have significantly more severe consequences for those users.

No research or analysis was conducted on access to the internet using mobile networks (using a 3G or higher method of data access) from handheld, usually mobile phone devices. There are additional risks associated with using these systems since there is often more direct control by monitoring and blocking agents of the state to monitor and intercept such communications. Many handsets do not support modern methods of encrypted communications, and the range of choices is severely restricted for users in this environment. More research in this area is required.

Recommendations

This report was written for internet users living under oppressive regimes, and for Freedom House and all others active on behalf of those users. This report also aims to improve an understanding of the important role and work of circumvention tool developers and how each tool is used around the world today to protect citizens and activists in a variety of complex situations.

Users

It is strongly recommended that users carefully plan their internet access needs according to their internet usage and risk profile, and the nature of the regime they live under. These regimes differ in the content they block and, perhaps the more importantly, in the way they deal with persons who breach state blocks and access or even produce such content.

According to the analysis conducted in this report, they should carefully choose the internet circumvention tool to be used, and should analyse the different risks between accessing and producing or distributing content. Those with limited needs for security and privacy, or those in more liberal or over-stretched regimes, may be better off using faster, often less secure tools, whereas others will want the safety of a portable or even web-based tool that leaves no traces and still provides strong encryption.

Although this report provides insight into the tools and their characteristics, it does not cover the detailed nature of the countries involved, nor the content that would be particularly sensitive in the regimes that enforce internet blocking and censorship schemes. The diagram on page 13 should provide guidance on this trade-off.

Users must be aware of other aspects of computer and network security to protect their activities online. It is important to remember that circumvention tools are not always designed with privacy and security in mind. The user may still be traceable as a user of circumvention

tools; the tool will only make it harder to link the user to specific content that was visited.

Computer systems need to have the latest software patches available from verified original software suppliers (software patches can be tampered with from other sources). Systems require anti-malware software with up-to-date definitions installed daily. A range of such tools can ensure broader protection from a wider range of malware software, including viruses, spyware, and Trojan attacks. Authorised users should have separate strong passwords on the computer. System and data disks should have encryption software⁶³ installed and in regular use, and all external USB-based key storage should also be encrypted.

Fundamentally, the computer should be physically protected at all times, preventing and ensuring unauthorized access from unwanted intrusion. Once physical access is gained by non-authorized persons, the system can no longer be considered secure. For complete security, travelling activists should never leave a computer in hotel room, including a hotel safe. Safety and security must become a way of life for activists who live in these regimes.

Circumvention Tool Developers

Circumvention tool developers are first invited to take note of the results of the technical testing conducted for this report. Some of these tools have shortcomings that could be repaired in future versions (or might already be in the development cycle). We would be please to receive notifications of any software updates or perhaps even errors in the analysis conducted.

Usable solutions are not only those that perform functional tasks well and are able to educate users about the inherent choices they make when selecting one type of tool over another. Usable solutions are those that have training materials and community support forums

63 One example is truecrypt on www.truecrypt.org.

adequate for different target audiences and have access to a well-designed user interface.

Privacy and confidentiality regarding the use of circumvention technologies create substantial technical challenges that deserve further research and investment (in terms of time and monetary resources). Circumvention tools need to look into the technical mechanisms to conceal the fact that circumvention technology is in use. Privacy and circumvention tools do not necessarily have the same objective. Users have the right to be informed about what personal identifiable information is provided by the operator of the circumvention technology infrastructure and what can be discovered from a forensic analysis of the computer or device being used.

Future Work

Regular repeated testing of these tools, both in-country (where feasible) and in a technical laboratory environment, is essential.

A significant number of lessons were learned from the work to create this report, and these experiences will enable future evaluation efforts to be even more robust and beneficial for users in the countries involved. In addition to regular repetition of this evaluation exercise, it would be useful to focus more on the attitude and requirements of internet users living under oppressive regimes. While they may be helped by this regular evaluation, it has become clear that a number of other environmental and regional parameters are involved when choosing if, where, and how to access sensitive speech, or of even greater concern, disseminating such content.

It is advisable that greater thought be given to a more user-centric manual or security guide that takes into account the results of the technical survey at hand and also the characteristics of the regime and the predominant access methods available. This security manual could then provide a more holistic and useful guide for users with limited internet freedom.

Multinational software development companies and mobile handset suppliers should be approached for technical and financial support to develop democracy-enhancing tools, blocking circumvention tools, and software protection utilities for use under oppressive regimes.

Glossary



Glossary

Anonymity

In security terms, anonymity means that it is not possible to identify specific internet users from the total user population. Ultimately, anonymity depends on how large the user population is, or how unique/similar one user is to the total population. The level of anonymity depends on what specific details need to be protected and from whom.

Confidentiality/Privacy

The term confidentiality implies ensuring that information is available only to those authorized to have access. It is different than anonymity because in confidentiality the data is available but restricted.

Technology could guarantee that the data is sent confidentially but often cannot hide the fact that certain tools are being used, often linking the author to the use of certain software.

Deep-Packet Inspection

A filtering and blocking technology that allows its user to see inside the contents of every packet traversing the wire. It can be used to filter or block content based on the contents of the communication, rather than on the address or URL being requested.

Pseudonyms

The use of an alternative identifier. Pseudonyms allow the user to have an alternate identity while using email, social networking tools or posting materials online.

Proxy Servers

Computer servers that allow remote access from nodes to content.

Many circumvention tools make use of well-known standard mechanisms to tell a web browser that traffic should be sent via a trusted third party server.

While HTTP proxy servers work specifically for HTTP connections, SOCKS is a general-purpose technology that allows many other applications to instruct a third

party server to open connection to certain destination and service.

Common circumvention tools will install a local proxy or a SOCKS server in the client machine. Traffic is then tunnelled elsewhere (see below).

VPN / Tunnelling software

Tunnelling software uses the technical principle of traffic encapsulation. Encapsulation of traffic means that the requests do not travel directly to the final destination but are tunnelled to an intermediary server. The intermediary server operates as a gateway between the end user and the global internet. This is similar to a proxy server. The main difference between a proxy solution and a tunnel solution is the way the traffic reaches the intermediary.

When using tunnels, you can think as if your secret letters travel inside of a sealed box. When the sealed box arrives at a post office, the box is opened and the letters are then distributed to the final destination. By sending the data (your letters) inside of sealed box (the tunnel), we are able to hide the final intended recipients from our attacker. We can, however, follow the box to the postoffice.

Such tunnelling software that encapsulates all traffic is commonly known as virtual private network (VPN).

Web-based circumvention systems

Web-based circumvention systems are based on the concept that users do not request the pages directly but use an intermediate website to request and display the content on their behalf, i.e., the third party acts as a proxy of the user. They are easy to use, they do not require additional software to install, and they normally have good performance in terms of speed.

To ensure confidentiality of the requested content and a secure identification of the circumvention webserver, the webserver often implements SSL or TLS connections (encrypted connections).

Appendices



Appendix 1

Methodology

This section describes the methodology used in this report. First, the different criteria for assessing the technical functionalities of different tools are outlined. Then, the survey mechanism is explained.

Technical Assessment Methodology

This report presents the result of a comparative review of the most popular initiatives in the area of privacy-enabled circumvention tools. The authors are aware that comparing different technologies and projects is a very complex task. Therefore, and in order to increase the objectivity of this exercise, a comprehensive methodology is developed here.

This analysis examines each tool based on the three aspects of usability, privacy and security, and transparency and sustainability. The first challenge here is to narrow down and produce a minimal, and yet sufficient, set of criteria that the average internet user could understand and relate to.

One of the aims of this report is to stimulate the debate in order to improve these technologies and acknowledge the current limitations of existing solutions when deployed in certain countries. When searching for tools to access blocked content, it is crucial that internet users understand what level and type of information is protected, from whom, and at what cost. Providing tools and technologies to protect internet users from surveillance (anonymity) or internet blocking (anti-circumvention) is not a simple task. As technology becomes ever more complex, a marketing pitch tends to exaggerate the problems or oversimplify the solutions. While academics tend to develop systems that very few can use, businesses are looking for bullet-proof solutions that can promise the impossible of absolute security. Absolute security and ultimate privacy on the internet are difficult to provide, especially because they are

properties that depend on the resources available to the adversary. Tools and technologies are difficult to compare, concepts are frequently misleading, and in-depth information is frequently missing. No matter what core technology is used, from the simple web proxy to the more advanced tunnel based solutions, the underlying concept remains the same: the traffic must be sent back and forth via a channel that is not blocked, while ensuring that the content is confidential and the third party servers remain unobservable as long as possible.

Building an infrastructure that supports circumvention while preserving using privacy is full of challenges, which we examine here through the use of three general categories of aspects of circumvention tools: usability; privacy and security; and performance.

Usability

Assessing the usability of the tools is to ensure that the technology is easy to use, and that the perceived benefits outweigh the additional complexities of using the internet. The following criteria were evaluated in this category:

- **Price:** Some circumvention tools are available for free, while others have premium services that require a user to pay for usage of the service. While the latter approach may lead to a more sustainable business model, a fully free service is preferable in countries where internet access is blocked; one never knows if the service will be blocked too, for instance. We have assessed whether the tool is paid, has premium service for a fee, or is generally free to use.
- **Availability:** Some tools are designed to grant access to the circumvention service only from within countries where blocking is highly pervasive, such as China and Iran. Others can be used globally. We have assessed how available tools are, granting higher scores for global or high availability.

- **Accessibility (portability):** Popular circumvention tools are quickly blocked in countries that apply internet filtering. How then can the software be accessed and downloaded among blocked users? Some tools work without client application (for example, they rely on server side application only). This approach is a great advantage in terms of accessibility. As another approach, a small tool can be mailed or transferred via the internet from one user to another, while larger ones might need to be passed on via a portable USB drive. In our review, we looked for tools that are easy to distribute.
- **GUI:** Although preferences towards the look of a tool (GUI stands for Graphical User Interface) may be of little concern to a casual user, it is important that to note that a more transparent GUI will prevent mistakes, and helps users to understand the tool better. We have assessed the GUI for this factor.
- **Documentation:** Documentation should cover at least what the tool does, how the tool works, what the known limitations of the tool are, and why anyone should use it. The number of languages in which it is offered is also considered.
- **Localization:** To facilitate worldwide usage, documentation and graphical user interface of the tool should be localized to relevant languages. In our review, we looked for tools with proper multilingual graphical interfaces and extensive documentation. While official documentation is a must, we also payed special attention to the existing unofficial documentation, including community contributions, discussion forums, and mailing lists.
- **Applications supported:** While some tools were designed to allow web-surfing only, many have support for other tools built in, allowing user unrestricted usage of service such as email and instant messaging directly from the client, without the need for specialist settings or other intermediate steps that would make the tool prone

to configuration errors. We assessed the number of tools supported without intermediate steps to access the tools access capabilities.

Privacy/Security

Assessing the privacy and security of the tools is an attempt to ensure a maximum level of privacy to the users. The ideal case will allow the users of the technology to remain anonymous and would make the requested content not traceable to any particular user. The following criteria are evaluated in this category:

- **Portability:** Software that does not need to be installed on a computer, but can run from a single executable file or even from an external flash drive, provides more flexibility than the ones that require installation. It is easier to hide the existence of software with high portability than one that is installed on a computer. In this review we looked for tools that do not leave traces during operation and after being uninstalled.
- **Applications:** Most circumvention tools focus mainly on web traffic, but there are also tools that allow the routing of other protocols inside the proxy network. Support for mail, instant messaging (IM), and file transfer protocols makes a tool more flexible. This review searched for tools that effectively support more types of internet applications.
- **Logging practises:** It is important to determine what information is stored in the proxy that is handling the requests. This also includes whether or not IP addresses and the requested URLs are logged. For tools that do maintain such user activity logs, it is also important to determine for how long these logs are preserved, and under which policies they are accessible to third parties. Naturally, a circumvention tool should log as little information as possible, and users should find a way to know what is logged, for what purpose, and for how long. In this review, we

looked for tools that have clear logging policies and correctly inform users about such practices.

- ▶ **Anonymity:** For the purpose of our technical test we have defined anonymity as a crypted channel to relatively anonymous IP being used. In other words, where the access method involves a crypted channel that cannot be easily intercepted and where accessing services is done from a relatively anonymous IP we have assumed that the user can stay relatively anonymous.
- ▶ **Tool Fingerprints and plausible deniability:** We have assessed whether a tool leaves tell-tale signs of its operation or installation on the computer of the user after use and un-installation. Where this is not the case and the tool is also portable, we have further assessed whether the tool, given many other aspects, would be likely to provide an excuse of “plausible deniability” to the user while not in use, meaning a user can safely deny the existence or usage of the tool when confronted with a situation where such a denial would be required.
- ▶ **End-user privacy:** An important aspect of circumvention tools is the ability to hide where the initial request came from. This can be done by creating a crypted channel to a relatively anonymous IP address. The crypted channel here will add to user privacy as communications cannot be easily intercepted. Also, it will be hard to hide the fact that circumvention tools are used while a connection is active and under surveillance, but where the tool does not have to be installed, added privacy is created: users can deny the use of such tools or hide their use more easily. We have therefore rated tools that provide both functionalities higher in our assessment of the security and privacy of the tool.

Performance

Assessing the performance of the tools is geared towards ensuring that the technology itself and the software implementing it are sufficiently functional to allow for effective internet usage. The following criteria were evaluated in this category. Please note that operating speed was not tested since this will be highly dependent on the countries internet access infrastructure.

- ▶ **Likely availability:** Proxy-based circumvention tools route internet traffic through one or more intermediaries (proxy servers) to retrieve the blocked content. These intermediaries can either be operated by the very same organization that develops the technology, or alternatively run by a third-party individual or organization. Major trust is delegated to those organizations operating the proxy servers. As a result, the individuals or organizations that operate the intermediaries will have to sustain the tools’ availability. In contrast with the technologies that use one single proxy, collaboration among all intermediaries is needed in order to track the IP address and the requests of a user in a multi-hop proxy solution or a P2P based solution. In this review we looked for tools that effectively use more than one intermediary so that availability, both in terms of resilience against blocking and against technical failures, is likely high. This criteria favours decentralized tools, as these are likely to have fewer points of failure.
- ▶ **Operating system:** Software that is supported on more than one platform covers a wider audience than solutions that can only run on one platform. In our review, we looked for tools that are multi-platform. A tool that also provides the possibility of running on mobile devices would have a clear advantage in this respect. The ability to run privacy-friendly circumventing tools on mobile devices is especially important in countries where 3G data networks are becoming more accessible in terms of price and availability.

- **GUI:** the Gui design is not only an indicator of usability but also of performance of a tools design team. We have included the GUI criteria in the performance section to highlight tools where ongoing development and investment in ease of use appears to be taking place.
- **Purpose built infrastructure and development:** Circumvention tools require long-term funding both in terms of infrastructure (proxy servers, bandwidth) and software development (updates, bug fixing, new features) to keep up with new demands. Resources normally come either from volunteers and donors or from an arrangement which would add profitability to the tool. Either way, where the business model of the tool is geared towards the purpose of circumvention, better long term results ought to be expected, while other tools, currently used to circumvent, may be rendered useless as time goes by. We have therefore assessed whether a tool was built for the purpose of circumvention and created the tools accordingly.
- **Start-up:** we have assessed whether a tool is quick to start up and whether usage can start instantly or requires a burdensome installation and/or payment.

Technical Test Environment

The length of this report does not allow for a detailed and comprehensive description of the experimentation procedure which has been used in this study⁶⁴ for each specific tool tested. As a compromise, here, the test environment and the utilized method are briefly described.

The evaluation of the different tools included in this report has been performed on two Linux boxes running

Ubuntu 8.04 LTS and Virtualbox virtualization software. Microsoft Windows XP was installed as guest operative system of the Virtualbox. During the month of March 2010, each of the tools was tested individually in an independent instance of Microsoft Windows XP with the latest software update and service packs having been installed prior to the tests.

In order to monitor what changes each tool performed in the operative system, two powerful tools from Microsoft System internals: Process Monitor⁶⁵ and TCPView⁶⁶ were used. Since Windows was running as guest operative system of Linux in a virtualized environment, some results could be verified by using the popular Linux packet sniffer Wireshark.

Tools can evolve quickly and technical testing is like fixing on a moving target and selecting a specific point in time. The technical tests and surveys for this report were conducted over a two week period in early Q2 2010. The websites hosting the tools were sampled in early 2011 to verify the tools were still available for download and use, and to confirm that no major upgrades had taken place which would negate the research conducted during Q2 2010. Minor changes were not taken into account. Sometimes, internal algorithms and implementations can be altered with minimal (if any) visual changes to the user interface or documentation and the effects of these alterations can only be determined by regular rigorous re-testing. Since network structures adapt and change rapidly in countries under complex political circumstances, understanding evolving blocking practises and strategies requires further resources and ongoing sampling of country based data.

The scores resulting from the technical tests were divided into the three main categories:

1. **Ease of Use**
2. **Performance**
3. **Support and Security**

⁶⁴ Where appropriate some specific details have been intentionally omitted from this report in order to avoid abuse of sensitive information by organizations involved in establishing internet filtering systems.

⁶⁵ <http://technet.microsoft.com/en-us/sysinternals/bb896645.aspx>.

⁶⁶ <http://technet.microsoft.com/en-us/sysinternals/bb897437.aspx>.

The scores for individual tests were then averaged to create a scale of 1 to 5 on which the tools were rated. We have created both category and overall scores for the tools. One characteristic of the technical methodology is that no tool would normally score less than two points for an individual aspect, unless the aspect was completely lacking or failing.

Survey Methodology

The surveys in the target countries are all based on the same set of questions initially developed in English. These questions, and the sets of options defined for each one of them, were translated into each one of the target languages and the link to the surveys is dispatched to prospective users through different social networks. Subsequently, the responses of the audience of the surveys are translated back to English and the same analysis is done on the sets. This section first describes the questions contained in the questionnaire. Then, the procedure carried out in each country is explained in detail.

Whereas the surveys created were distributed across a wide network of contacts in each target country, due to the nature of the target environments and the need for security, it was not possible to achieve rigorous survey sampling. It is important to note that the survey results are not intended as a rigorous statistical sampling in these countries. The voluntary responses received are instead treated as indicative of in-country user experiences. The combined use of the technical analysis and the country surveys creates interesting and challenging points for comparison and reflection.

The purpose of the survey is to determine how the tools perform from a user's point of view, recognising that such tools are used in different countries under different Internet blocking regimes. Different tools will be adopted by users in different countries based on experience, expectations, privacy requirements, intuitive and technical gossip of blocking technologies in use, the urgency and types of communications and the internet

network architecture in each country. For example, reading online public sources of banned publications might require one type of tool to bypass internet blocking systems whereas publishing information considered restricted would be more dangerous for the person involved and therefore require tools with higher levels of safety and privacy.

Questionnaire Structure

The in-country survey consisted of two parts. The first part asked general question about the country, the user skill level and several general background facts related to the study. The second part held questions regarding the tools and their usage in the country at hand.

In the first part, the user is asked for the country and the type of place from which they primarily access the internet. The different options for where a user normally connects to the internet include public places, work computers, and personal computers. Then, the user is asked about the type of Internet connection they normally use, and their assessment of their skill level. The following six questions in this part directly address the issue of filtering and the interaction of the users with the circumvention tools. Starting from how often the user encounters blocked websites, the user is asked about how they learned about the circumvention tools covered in the questionnaire, and how they would acquire them. This part concludes with the two questions regarding the first and the second most important features for the user when they choose a circumvention tool.

The second part of the questionnaire surveys the users experience with the different tools which were evaluated in this report. The survey questions are divided into three categories. These categories are:

- 1. Category A: Ease of Use**
- 2. Category B: Performance**
- 3. Category C: Support and Security**

Some users may have sufficient technical knowledge to evaluate computer software tools and other users may have basic knowledge such that the user has adequate knowledge to install or configure their computer systems to use these tools. The survey is not designed to test the user's skill level (which is self-assessed in one question in the first section of the survey) but focuses on the subjective experiences of using the different tools in the different regimes. The analysis of the results of this survey is designed to offer a second means of evaluating the tools tested in the technical testing section. This subjective but real life testing is designed to complement the results of the technical testing and enable the developers to understand the needs and requirements of users in the different countries.

Country Survey Implementation

The survey was implemented in different ways in each country.

Azerbaijan

The survey for Azerbaijan was conducted offline, due to very high security restrictions and low internet penetration. Because it was not possible to conduct the survey publicly, the surveyors targeted human rights and pro-democracy activists, especially those at technical trainings on how to use circumvention tools and other workshops.

Burma

The survey for Burma was conducted offline, due to very high security restrictions and low internet penetration. Because it was not possible to conduct the survey publicly, the surveyors targeted human rights and pro-democracy activists, especially those that have received previous technical trainings on how to use circumvention tools.

China

The survey for China was conducted online using a Google docs application that collects surveys

results, as more common online survey tools (such as SurveyMonkey) are blocked. The survey was promoted via links posted on Twitter and other social networking platforms through popular netizens and bloggers in China. Using a data aggregation available on the Google platform, the surveyors then aggregated the responses. Because of the unique internet censorship situation in China, the surveyors included additional tools in the questionnaire, such as Puff and SSH, since many internet users use these solutions as well.

Iran

The Persian (Farsi) translation of the survey was hosted on Google Documents and the link was sent out on Twitter, Google Reader, Facebook, and FriendFeed. A post was published on a well-known site as well, in order to encourage Persian bloggers and blog-readers to participate in the survey. Well-known figures in the Persian blogosphere recommended the survey to others through sharing the link in different social networks.

Appendix II

Survey Questionnaire

QUESTIONNAIRE: PRODUCT REVIEW OF CIRCUMVENTION TOOLS AND METHODS

Review Objectives

- The objective of the product review is to assess how well different tools work in countries where internet censorship is pervasive or at least common. The review will assess the following features of the tools: ease of use; performance; ability to receive support for the tools; and security.
- This product review will be anonymous.
- Scoring: The overall categories will be rated on a scale from 1 to 5, with 5 being the best score (most helpful in circumventing censorship) and 1 the worst, (the least helpful in circumventing censorship).
- Tools under review:
 - Dynaweb
 - Freegate
 - Freenet
 - Garden GTunnel
 - Google (Translate, Reader, Cache, etc.)
 - GPass
 - Hotspot Shield
 - JAP
 - Proxy
 - Psiphon
 - RSS feeds
 - Tor
 - UltraSurf
 - Your Freedom
 - VPN
 - Other – please specify

Product Review Questionnaire Tools Review Part 1: Usage

- 1. From which country do you primarily access the internet?**
- 2. Where do you normally connect to the internet?**
 - Internet café or other public computer
 - Work computer
 - Personal computer/Mobile phone
 - Other – please specify
- 3. What type of internet connection do you normally use?**
 - a) Dial-up b) Broadband (DSL/Cable)
 - c) Satellite d) Other
 - e) Don't know
- 4. What is your skill level as an internet user?**
 - Beginner (email, basic internet browsing)
 - Intermediate (blogging, social networking online)
 - Advanced (programming)
- 5. When you use the Internet, how often do you encounter blocked websites?**
 - 1) Always 2) Often 3) Sometimes
 - 4) Rarely 5) Never 6) Don't know
- 6. How did you learn about the abovementioned tools (please evaluate each tool separately)?**
 - Friend/colleague
 - Over the internet
 - Via an email that was sent to me
 - Other – please specify
- 7. How do you acquire the majority of the tools you use?**
 - a) Website b) Email c) USB/DVD/CD
 - d) Other – please specify
- 8. How often do you use the abovementioned tools (please evaluate each tool separately)?**
 - 1) Always 2) Often 3) Sometimes
 - 4) Rarely 5) Never
- 9. Which is the most important to you in choosing a circumvention tool?**
 - Ease of use
 - Speed
 - Support, if I have questions or need help
 - Anonymity/security
 - Other – please specify
- 10. Which is the second most important to you in choosing a circumvention tool?**
 - a) Ease of use b) Speed
 - c) Support, if I have questions or need help
 - d) Anonymity/security e) Other – please specify

Product Review Part II: Categories and Questions

Category A: Ease of Use

11. Ease of finding: How easy is it to find the abovementioned tools?

(please evaluate each tool separately)?

- 5) Very easy 4) Fairly easy
- 3) Neither easy nor difficult
- 2) Fairly difficult 1) Very difficult
- 0) Not Applicable

Tool	Easy				Hard	n/a
Dynaweb	5	4	3	2	1	0
Freegate	5	4	3	2	1	0
Freenet	5	4	3	2	1	0
Garden GTunnel	5	4	3	2	1	0
Google (Translate, Reader, Cache)	5	4	3	2	1	0
GPass	5	4	3	2	1	0
Hotspot Shield	5	4	3	2	1	0
JAP	5	4	3	2	1	0
Proxy	5	4	3	2	1	0
Psiphon	5	4	3	2	1	0
RSS feeds	5	4	3	2	1	0
Tor	5	4	3	2	1	0
UltraSurf	5	4	3	2	1	0
Your Freedom	5	4	3	2	1	0
VPN	5	4	3	2	1	0
Other – please specify	5	4	3	2	1	0

12. Ease of operating: how easy is it to work with abovementioned tools?

(please evaluate each tool separately)

- 5) Very easy 4) Fairly easy
- 3) Neither easy nor difficult
- 2) Fairly difficult 1) Very difficult
- 0) Not Applicable

Tool	Easy				Hard	n/a
Dynaweb	5	4	3	2	1	0
Freegate	5	4	3	2	1	0
Freenet	5	4	3	2	1	0
Garden GTunnel	5	4	3	2	1	0
Google (Translate, Reader, Cache)	5	4	3	2	1	0
GPass	5	4	3	2	1	0
Hotspot Shield	5	4	3	2	1	0
JAP	5	4	3	2	1	0
Proxy	5	4	3	2	1	0
Psiphon	5	4	3	2	1	0
RSS feeds	5	4	3	2	1	0
Tor	5	4	3	2	1	0
UltraSurf	5	4	3	2	1	0
Your Freedom	5	4	3	2	1	0
VPN	5	4	3	2	1	0
Other – please specify	5	4	3	2	1	0

13. Ability to function in different languages: How well do the abovementioned tools function in the language that you use the most online?

(please evaluate each tool separately)

- 5) Very easy 4) Fairly easy
- 3) Neither easy nor difficult
- 2) Fairly difficult 1) Very difficult
- 0) Not Applicable

Tool	Easy				Hard	n/a
Dynaweb	5	4	3	2	1	0
Freegate	5	4	3	2	1	0
Freenet	5	4	3	2	1	0
Garden GTunnel	5	4	3	2	1	0
Google (Translate, Reader, Cache)	5	4	3	2	1	0
GPass	5	4	3	2	1	0
Hotspot Shield	5	4	3	2	1	0
JAP	5	4	3	2	1	0
Proxy	5	4	3	2	1	0
Psiphon	5	4	3	2	1	0
RSS feeds	5	4	3	2	1	0
Tor	5	4	3	2	1	0
UltraSurf	5	4	3	2	1	0
Your Freedom	5	4	3	2	1	0
VPN	5	4	3	2	1	0
Other – please specify	5	4	3	2	1	0

Category B: Performance

14. Scope: Of the blocked websites, the abovementioned tools allow you to access?

(please evaluate each tool separately)

- 5) All websites 4) Many websites
- 3) Some websites 2) Few websites
- 1) No websites 0) Not Applicable

Tool	All	Hard	n/a			
Dynaweb	5	4	3	2	1	0
Freegate	5	4	3	2	1	0
Freenet	5	4	3	2	1	0
Garden GTunnel	5	4	3	2	1	0
Google (Translate, Reader, Cache)	5	4	3	2	1	0
GPass	5	4	3	2	1	0
Hotspot Shield	5	4	3	2	1	0
JAP	5	4	3	2	1	0
Proxy	5	4	3	2	1	0
Psiphon	5	4	3	2	1	0
RSS feeds	5	4	3	2	1	0
Tor	5	4	3	2	1	0
UltraSurf	5	4	3	2	1	0
Your Freedom	5	4	3	2	1	0
VPN	5	4	3	2	1	0
Other – please specify	5	4	3	2	1	0

15. Consistency: How often do the abovementioned tools enable you to access blocked websites?

(please evaluate each tool separately)

- 5) Always 4) Most of the time
- 3) Sometimes 2) Rarely
- 1) Never 0) Not Applicable

Tool	Always	Never	n/a			
Dynaweb	5	4	3	2	1	0
Freegate	5	4	3	2	1	0
Freenet	5	4	3	2	1	0
Garden GTunnel	5	4	3	2	1	0
Google (Translate, Reader, Cache)	5	4	3	2	1	0
GPass	5	4	3	2	1	0
Hotspot Shield	5	4	3	2	1	0
JAP	5	4	3	2	1	0
Proxy	5	4	3	2	1	0
Psiphon	5	4	3	2	1	0
RSS feeds	5	4	3	2	1	0
Tor	5	4	3	2	1	0
UltraSurf	5	4	3	2	1	0
Your Freedom	5	4	3	2	1	0
VPN	5	4	3	2	1	0
Other – please specify	5	4	3	2	1	0

16. Speed: How quickly are the abovementioned tools in accessing blocked sites?

(please evaluate each tool separately)

- 5) Very fast 4) Fairly fast
- 3) Neither fast nor slow 2) Fairly slow
- 1) Very slow 0) Not Applicable

Tool	Fast	Slow	n/a			
Dynaweb	5	4	3	2	1	0
Freegate	5	4	3	2	1	0
Freenet	5	4	3	2	1	0
Garden GTunnel	5	4	3	2	1	0
Google (Translate, Reader, Cache)	5	4	3	2	1	0
GPass	5	4	3	2	1	0
Hotspot Shield	5	4	3	2	1	0
JAP	5	4	3	2	1	0
Proxy	5	4	3	2	1	0
Psiphon	5	4	3	2	1	0
RSS feeds	5	4	3	2	1	0
Tor	5	4	3	2	1	0
UltraSurf	5	4	3	2	1	0
Your Freedom	5	4	3	2	1	0
VPN	5	4	3	2	1	0
Other – please specify	5	4	3	2	1	0

Category C: Support and Security

17. Problems: How often have you encountered operational problems using the abovementioned tools?

(please evaluate each tool separately)

- 5) Always 4) Most of the time
- 3) Sometimes 2) Rarely
- 1) Never 0) Not Applicable

Tool	Always				Never	n/a
Dynaweb	5	4	3	2	1	0
Freegate	5	4	3	2	1	0
Freenet	5	4	3	2	1	0
Garden GTunnel	5	4	3	2	1	0
Google (Translate, Reader, Cache)	5	4	3	2	1	0
GPass	5	4	3	2	1	0
Hotspot Shield	5	4	3	2	1	0
JAP	5	4	3	2	1	0
Proxy	5	4	3	2	1	0
Psiphon	5	4	3	2	1	0
RSS feeds	5	4	3	2	1	0
Tor	5	4	3	2	1	0
UltraSurf	5	4	3	2	1	0
Your Freedom	5	4	3	2	1	0
VPN	5	4	3	2	1	0
Other – please specify	5	4	3	2	1	0

18. Solutions: When you have encountered a problem, how easy was it for you to obtain help?

- 5) Very easy 4) Fairly easy
- 3) Neither easy nor difficult
- 2) Fairly difficult 1) Very difficult

Tool	Easy				Hard	n/a
Dynaweb	5	4	3	2	1	0
Freegate	5	4	3	2	1	0
Freenet	5	4	3	2	1	0
Garden GTunnel	5	4	3	2	1	0
Google (Translate, Reader, Cache)	5	4	3	2	1	0
GPass	5	4	3	2	1	0
Hotspot Shield	5	4	3	2	1	0
JAP	5	4	3	2	1	0
Proxy	5	4	3	2	1	0
Psiphon	5	4	3	2	1	0
RSS feeds	5	4	3	2	1	0
Tor	5	4	3	2	1	0
UltraSurf	5	4	3	2	1	0
Your Freedom	5	4	3	2	1	0
VPN	5	4	3	2	1	0
Other – please specify	5	4	3	2	1	0

19. Support Validity: How frequently does the help you find come directly from the tool's developers or the tool's network?

- 5) Always 4) Most of the time
- 3) Sometimes 2) Rarely
- 1) Never 0) Not Applicable

Tool	Always				Never	n/a
Dynaweb	5	4	3	2	1	0
Freegate	5	4	3	2	1	0
Freenet	5	4	3	2	1	0
Garden GTunnel	5	4	3	2	1	0
Google (Translate, Reader, Cache)	5	4	3	2	1	0
GPass	5	4	3	2	1	0
Hotspot Shield	5	4	3	2	1	0
JAP	5	4	3	2	1	0
Proxy	5	4	3	2	1	0
Psiphon	5	4	3	2	1	0
RSS feeds	5	4	3	2	1	0
Tor	5	4	3	2	1	0
UltraSurf	5	4	3	2	1	0
Your Freedom	5	4	3	2	1	0
VPN	5	4	3	2	1	0
Other – please specify	5	4	3	2	1	0



1301 Connecticut Ave. NW, Fl. 6,
Washington, D.C. 20036

www.freedomhouse.org

designed by **catalysto**