

# Circumvention is not privacy!

## Evaluation and comparison of common Internet Circumvention Tools

Alberto Escudero-Pascual  
Stockholm, Sweden  
July 2010  
version 4.4

This working document contains a technical evaluation of eleven tools that are commonly used to circumvent Internet blocking. The review was conducted in March 2010 for the period of one month.

# Table of Contents

1	Executive Summary.....	1
2	Our motivation.....	2
3	Our methodology.....	3
4	From buzzwords to secure properties.....	3
4.1	Anonymity.....	4
4.2	Unlinkability.....	4
4.3	Undetectability and unobservability.....	5
4.4	Pseudonymity.....	5
4.5	Confidentiality.....	5
5	Digging underneath technology.....	7
5.1	Web-based circumvention systems.....	7
5.2	Tunneling software.....	7
5.3	Socks and Proxies.....	8
6	Challenges: from paper to sustainable implementation.....	8
7	Evaluation criteria .....	10
7.1	Sustainability.....	10
7.1.1	Funding of infrastructure and development.....	10
7.1.2	Accessibility.....	10
7.2	Trustworthiness.....	10
7.2.1	Transparency.....	10
7.2.2	Level of protection.....	11
7.2.3	Track record.....	11
7.2.4	Developers.....	11
7.3	Usability.....	11
7.3.1	Documentation.....	11
7.3.2	Localization.....	11
7.3.3	Access to software .....	12
7.3.4	Software updates.....	12
7.3.5	Operating system.....	12
7.3.6	Portability.....	12
7.3.7	Applications.....	13
7.4	Privacy.....	13
7.4.1	Target group.....	13
7.4.2	Logging practises.....	13
7.4.3	End-user privacy.....	13
7.4.4	Location Privacy.....	14
7.5	Infrastructure Development.....	14
7.5.1	Decentralized vs Centralized.....	14
7.5.2	Resilient.....	14
7.5.3	Speed.....	15
8	Tools Evaluation.....	16
8.1	Dynaweb.....	16
8.2	Freegate.....	17
8.3	GTunnel.....	18
8.4	Gpass.....	19
8.5	Google (reader, translation, cache).....	20

8.6 Hotspot shield.....	21
8.7 JAP.....	23
8.8 Phisphon.....	24
8.9 Tor.....	25
8.10 Ultrasurf.....	27
8.11 Your Freedom.....	28
9 Our testing laboratory.....	29
10 Recommendations.....	30
11 Tools Comparison Matrix.....	31

## **1 Executive Summary**

As a result of the multiple attempts to block the content in the Internet, several projects that fall under the category of circumvention technologies has become widely spread.

Circumvention tools are primarily designed to bypass Internet filtering, the core principle behind the technologies is to bounce the connections using one or more collaborative servers.

This report offers a technical review of ten different projects and a practical methodology to evaluate them. The review aims to make accessible an area of knowledge for those interested in circumvention but not necessary enjoy reading dozen of acronyms or installing all the tools available.

One of our first findings performing this review is that comparing the initiatives has not been a simple task, developing a simple evaluation criteria is far from straightforward and many solutions are black boxes that require reverse engineering to gain understanding of their functionality. We have accepted the challenge to develop a digestible methodology that looks at the tools under five basic categories: sustainability, trustworthiness, usability, privacy and infrastructure. As a result of the evaluation we have identified twenty criteria that can be used to assess the suitability of a tool.

Our major finding is that tools designed for circumvention are not necessary suitable for privacy protection and there is not enough awareness about the risk involved in using technologies that can be easily spotted.

A major recommendation of this work is that investments in this area should focus on suitable business models, usability and ultimately technical solutions that can scale up taking advantage of peer-to-peer infrastructures. Not all users need to hide their use of circumvention tools but those *who are and live at risk* should be fully aware of what circumvention tools can and can not provide.

## 2 Our motivation

Although the Internet is rapidly becoming the global unified communication network, it was not originally designed to fully preserve certain types of privacy. Accessing and publishing content while ensuring proper confidentiality it is not just a technical challenge but a controversial area of discussion that awakes passionate legal and social debates.

With or without the Internet and all its powers, the ultimate questions still remain: What level of anonymity is desirable in our societies? How simple should be for an average person to access certain types of technologies? What is the right balance between anonymity and accountability? Who is responsible of building and paying for a privacy friendly telecommunication infrastructure?

Back in 1993, The Finnish developer Johan Helsingius created what is probably the first widely-used system to send anonymous e-mails. The system, known as the *Penet remailer* operated for three years and reached 700.000 registered users. It should not be a surprise for anyone that such system suffered from both technical and legal problems. Ultimately, *Penet* was shutdown in 1996 but it remains as a good example of the difficulties to balance *freedom of information* with *social accountability*.

Another major attempt to provide such infrastructure took place between 1997 and 2001, when the Canadian company Zero Knowledge Systems operated the *Freedom Network*, a global network of servers enabling private and secure Internet surfing. Although the company assembled an excellent group of cryptographers and Internet networking experts that was enough to convince customers to pay for the services. The project was shut down due to the ongoing high cost and limited economical returns of operating the network.

Two decades after *Penet* and one decade after the *Freedom Network*, there are still dozen of projects aiming to ensure that content on the Internet remains widely available while providing certain levels of privacy.

This report presents the result of a comparative review of the most popular initiatives in the area of privacy enabled circumvention tools. We are aware that comparing different technologies and projects is a very complex task so we have developed a comprehensive evaluation criteria that could allow us to undertake this work.

Comparing some of the solutions has been as easy as comparing apples and oranges (pears) but eventually we have come up with five major attributes to look in: infrastructure, privacy, usability, sustainability and trust.

Our ultimate goal is to write an accessible document to an audience that wants to know more about existing Internet circumvention tools and choose what suits better their needs.

### **3 Our methodology**

One of our first findings while looking into other existing reviews of circumvention tools was the lack of a comprehensive framework to address this task. Security is a vast area and claiming that one tool is more secure than another is like saying that driving in Reykjavik is better than having holidays in Madrid. Bold statements have no value without proper contextual information and justification.

Providing privacy while ensuring that all content remains available it is not simple challenge. Technology needs to be designed for common users but oversimplifying can expose users to life risking consequences.

Our first challenge was to narrow down what we were looking into and try to find a limited set of criteria that a normal reader could understand without the need of completing computer security graduate studies. It is a fact that a “chain is no stronger than its weakest link”, and that computer scientists and users point each other as main responsible of dysfunctional software.

This document starts by introducing a set of common security terms [Section 3] and core technologies [Section 4] that are frequently used in this review. Before providing a review of each of the tools [Section 6] you can read about the evaluation criteria that we had in our mind [Section 5].

We have not forgotten those that are technically curious about our technical setup and the tools involved in our assessment (geeks!) and we have included a section describing our testing environment [Section 6].

A report like this one can not finish without a summary of recommendations and findings [Section 7]. Ultimately, we want to stimulate a debate to improve these technologies and acknowledge the current limitations of existing solutions when deployed in certain countries.

### **4 From buzzwords to secure properties**

The first challenge that a computer user finds when looking for tools to access blocked content is to really 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 gets more complex, marketing pitch tends to exaggerate the problems or oversimplify the solutions. While academics tend to develop systems that very few can use, business are looking for bullet proof solutions that can promise the impossible: absolute security.

It is a know fact that the human is the weakest part of any system<sup>1</sup> and while tools can

---

<sup>1</sup> An open research question is if a computer security scientist is a human.

help, awareness and education can not be replaced easily by technology.

Absolute security and ultimate privacy in Internet are difficult to provide, specially 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 frequently missing.

Let start by trying to run away from buzzwords and provide a few concepts that are relevant to this topic so it is much easier to compare tools and technologies.

## **4.1 Anonymity**

From the point of view of an attacker, *anonymity* means that the attacker cannot identify a subject from the “crowd”.

The first important concept to remember when it comes to anonymity is the ability of not to stand out from the rest<sup>2</sup>. Ultimately, anonymity depends on how big is the crowd around you, or how similar you are from the rest of people. Think how easy will be to identify a person that drives a Batmobile in a Masai market in Arusha!

**[ILLUSTRATION: A Batmobile in a Masai market]**

*Anonymity* depends on what information needs to be protected.

Let us consider the scenario when a person opens its laptop one hour before boarding a plane in an airport. Consider how different are the scenarios when the attacker is trying to find out who is using a computer in an airport or if the information of interest is to find out who is posting “certain article” from the airport. Before looking for a tool, ask yourself the question “What is the information that needs to be protected?”

The second concept to remember is: “What is the attacker trying to find out? - What is the information that you need to protect?”

## **4.2 Unlinkability**

Another of those techie words is *unlinkability*. We consider that two or more things or events are unlinkable when our attacker can not distinguish if there are related or not.

Let us consider again our previous scenario of a person using a laptop from an airport. Can the attacker determine if certain content was posted by that person?. Is there any evidence available to the attacker to link the fact that a person was at the airport using a laptop and that certain article was posted in a website?.

---

<sup>2</sup> In Scandinavia, this is commonly referred in society as following the “Jante law”, where an individual is not allowed to be different from the others.

[ILLUSTRATION: A person with a laptop posting an article,  
someone watching from the distance]

### **4.3 Undetectability and unobservability**

The term *undetectability* refers to the possibility of distinguishing if certain event exists or not.

If we consider that certain article is posted in a website our main interest, we can say that the posting is undetectable if the attacker can not determine if the posting took place or not from the airport.

But imagine if the interest of the attacker is not to detect the posting but rather to detect who is using certain set of software tools. It is perfectly possible that while the posting itself is *undetectable*, the fact that someone was using certain technology is not.

The term *unobservability* goes one step further and it is used to describe the scenario where not only the item of interest is *undetectable* but also the parties involved are *anonymous*.

In our airport scenario, *unobservability* implies that the attacker can not detect that the article has been posted and at the same time the sender and receivers of the posting remain *anonymous*.

### **4.4 Pseudonymity**

Sometimes it needed to strike a balance between full anonymity and accountability. The use of *pseudonymity* allows you the possibility of using an alternative identifier (think in a nick name here!) other than one your real name.

[ILLUSTRATION: Superman and Clark Kent]

*Pseudonymous identifiers* allows us to have a alternate identity while sending mail or posting an article in a website.

### **4.5 Confidentiality**

Finally the term confidentiality implies to ensure that information is available only to

those authorized to have access.

Let us imagine that our attacker want to identify the content and authors of the articles that are sent from the airport. Confidentiality implies that our attacker can not access the content and authors of such articles.

As you can see there are many properties that can or can not be achieved during a very simple event. The possibilities are endless, the attacker might be interested in knowing what language the articles are posted, what kind of operative system the author uses or how many people are behind certain set of postings.

Technology could guarantee that the article is sent confidentially but maybe we can not hide the fact that certain tools are being used, linking the author to the use of certain software. We can aim to protect our identify using a pseudonym or put all our energy in making the posting undetectable.

What is important to understand before looking for any technology solutions labeled as circumventions tools is to what extend such technologies protect the identity of their users. In an ideal world circumventing tools and privacy protection should go hand in hand. Unfortunately, circumvention is not privacy!

## 5 Digging underneath technology

### 5.1 *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 party to request the content on their behalf, i.e. the third party acts as a proxy of the user.

From a technical standpoint of view, the Web-based circumvention systems are the simplest technology to overcome Internet censorship. They are easy to use, they do not require additional software to install and they normally have good performance in terms of speed. The challenge for both the users and the attackers is to find out where those proxies are. The users can reach blocked content using the Web relays and the circumvention system remains functional as long as the attacker can not observe where the relays (proxies) are located.

Although there are a few technical variations of the same concept, the basic idea is that the user points his or her browser to certain “websites” in order to reach the information that is unreachable using a direct connection. The desired content is displayed within the intermediary webserver.

**ILLUSTRATION: Proxy. A straight path between two places, an alternative but longer path. Maybe a TOMTOM illustration?**

To ensure confidentiality of the requested content and a secure identification of the circumvention webserver, the webserver must implement properly SSL. Unfortunately, valid SSL encryption (valid X.509 certificates) are not widely used in web-based circumvention systems opening the possibility for an attacker to impersonate the server and observe both the requested content and identify the users connected to the system.

### 5.2 *Tunneling software*

Another type of circumvention technique uses the technical principle of *traffic encapsulation*. Encapsulation of traffic means that, as in the case of using a proxy, the requests do not travel directly to the final destination but are tunneled to an intermediary server. The intermediary server acts as the end of the tunnel and operates as a gateway of the data stream. 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 to 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 a sealed box (the tunnel), we are able to hide the final intended recipients from our attacker. Tunneling software can operate for all types of traffic or only for certain applications (web). The tunneling software that encapsulates all traffic is commonly known as VPN

(virtual private network) while web specific tunneling solutions are known as web tunnelling.

As in the case of proxies, there are several technical variations of tunneling. Some softwares use full IP encapsulation, others encapsulate just the web requests (HTTP) inside of other protocols. The important thing to understand is that tunneling is just another (more advanced) technical mechanism where traffic is routed to an intermediary before reaching the final destination.

### **5.3 Socks and Proxies**

Many circumvention tools make use of well known standard mechanisms to tell a web browser that the traffic should be sent via a third party server. The most common mechanisms to ask webpages to third parties are known as *HTTP proxying* and *SOCKS* (from the word sockets). While HTTP proxying works specifically for HTTP connections, *SOCKS* is a general-purpose technology that allows applications to instruct a third party server to open connection to certain destination and service. The latest version of *SOCKS*, known as version 5, supports any protocol including name resolution or voice services based on *UDP*.

Common circumvention tools will install a local proxy or a *SOCKS* server in the client machine and modify the settings, with or without user intervention, of the most common tools. By modifying the proxy/SOCKS settings of the client machine, traffic starts to travel via a non-blocked group of servers.

Most common tools combine a local *SOCKS* server with some tunneling mechanism. When your web browser requests a webpage, the traffic is routed first to a locally installed *SOCKS* server to later travel via a newly created encrypted tunnel towards one or several proxy servers.

## **6 Challenges: from paper to sustainable implementation**

No matter what core technology is used, from the simple web proxying to the more advance tunneling solutions, the underneath concept remains the same: send your traffic 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 circumventing while preserving using privacy is full of challenges, for the sake of simplicity we have classified the challenges in five major areas. The number of areas is completely arbitrary but it is highly inspired by cognitive psychologist George A. Miller. Miller's Law states that number of objects an average human can hold in working memory is 7 plus or minus two ( $7 \pm 2$ ). Here there are the five

areas that we are the focus of our evaluation criteria<sup>3</sup>:

1. **Sustainability:** ensure that solution including its technical development and required support infrastructure has a business model.
2. **Trust:** ensure that the technology itself and the parties involved are trustworthy.
3. **Usability:** ensure that the technology is easy to use and the perceived benefit is compensates for the extra complexity added to use the Internet.
4. **Privacy:** ensure a maximum level of privacy to the users, ideally the users of the technology remain anonymous and the requested content is not linkable to them.
5. **Infrastructure Development:** ensure that the infrastructure that routes the traffic is highly dynamic, affordable and can not be blocked easily.

---

<sup>3</sup> The evaluation criteria is also inspired by engineer Kelly Johnson that in the 50s made popular the “KISS principle”. The KISS principle (Keep it simple and stupid!) states that simplicity should be the key goal in any design and that unnecessary complexity should be avoided. Our evaluation criteria contains five areas that respond to the well known acronym S.T.U.P.ID (Sustainability, Trust, Usability, Privacy and Infrastructure Development!)

## **7 Evaluation criteria**

### **7.1 Sustainability**

#### **7.1.1 Funding of infrastructure and development**

Circumvention tools need long term funding both in terms of infrastructure (proxy servers, bandwidth) and software development (updates, bug fixing, new features) to keep up with new technologies. Resources normally comes either from volunteers, donors or from making some kind of profit (business) from the tool.

It is arguable which model is the most sustainable one, as volunteers can loose interest in a tool or grow to a large supportive community, donor funds can run out or be a part of a long term research project, business plans can fail or develop to a thriving business. In our opinion, the best alternative is to be flexible in terms of finding resources, have good connections over the world, and build a strong and loyal community around the tool.

#### **7.1.2 Accessibility**

Can the tool be used in your country, or is the service only available for users in certain countries?

In our review we were looking for tools that have a sustainable business model and a distributed and decentralized infrastructure.

### **7.2 Trustworthiness**

#### **7.2.1 Transparency**

A first and important step towards transparency is the openness of the source code. By letting anyone (security experts, software developers) review the source code makes the likelihood of security flaws less likely, and bugs can be detected and patched quicker than in closed-sources software.

Another aspect related to transparency is the underlying *technical principles* of a tool. How data is encrypted?, how the traffic is routed?, are open standards followed?, what, where and for how long personal information is stored? are just a few of issues that can be implemented in countless amount of ways. A well designed privacy friendly circumvention tool shall not depend on secrecy of its code, protocols, and technology in use.

### **7.2.2 Level of protection**

A trustworthy tool needs to provide clear specifications of what the software can do, and what it can not do. Bold statements are insufficient when trying to find clear answers for questions like: What level of privacy, anonymity, and unlinkability can be guaranteed? What types of attacks can the tool sustain? Which risks can a user expect from using the tool?

In our review we were looking for tools that rely on strong encryption algorithms, secure communication protocols and peer reviewed code.

### **7.2.3 Track record**

Has the tool been targeted previously by authorities? Does the tool operator have real field experience and can react promptly to technology developments?

A tool that has been around for several years, and still have a large community of users has probably a good track record of avoiding attempts to stop their service. New technologies tend to attract media attention but is that desirable in all scenarios?

In our review we were looking for tools that have a good track record adapting to new kinds of Internet filtering.

### **7.2.4 Developers**

Who are the developers behind the tool? What is their background and previous experience in the field of computer security and Internet privacy?

In our review we were looking for tools that have recognized security experts in their development teams.

## **7.3 Usability**

### **7.3.1 Documentation**

No matter how simple and intuitive a circumvention tool is, extra documentation never hurts. Documentation should cover at least: what the tool does, how the tool works, what are the known limitations and why anyone should use it.

### **7.3.2 Localization**

To facilitate worldwide usage, documentation and graphical user interface of the tool should be localized to relevant languages.

In our review we were looking for tools that have good and multilingual graphical interfaces and extensive documentation. While official documentation is a *must*, we are also paying special attention to the existing unofficial documentation including community contributions, discussion forums and mailing lists.

### **7.3.3 Access to software**

Popular circumvention tools are quickly blocked in countries that apply Internet filtering. So how can the software be accessed and downloaded among blocked users? Some tools work without client application (relied on server side application only), which is a great advantage in terms of accessibility. A small tool that can be mailed or transferred via Internet Messengering from one user to another, while larger ones might need to be passed on via a portable USB drive.

In our review we were looking for tools that are easy to distribute.

### **7.3.4 Software updates**

How are software updates handled? Are they automatic or do they involve manual intervention (download and install new version of software)? Are software updates easy to track?

In our review we were looking for tools that require very simple or no software updates.

### **7.3.5 Operating system**

Obviously, software that is supported on more than one platform cover a wider audience that solutions that can run in one platform.

In our review we were looking for tools that are multi-platform including the possibility to run in Mobile devices. The ability of running privacy-friendly circumventing tools in Mobile devices is specially important in countries where 3G data networks are becoming more accessible in terms of price and availability.

### **7.3.6 Portability**

A software that does not need to be installed in a computer, but can run from a single executable file or even from an external flash drive, provides more flexibility than those that require an installer. It is easier to hide the existence of a software with high portability, than one that is installed on a computer.

In our review we were looking for tools that do not leave traces during operation and after being uninstalled.

### **7.3.7 Applications**

Most circumvention tools focus mainly on web traffic, but there are also tools that allow route other protocols inside of the proxy network. Support for mail, instant messaging (IM) and file transfer protocols makes a tool more flexible and all round.

In our review we were looking for tools that effectively support any type of Internet applications.

## **7.4 Privacy**

### **7.4.1 Target group**

Some tools are known to be used for the circumvention of certain type of blocked content and serve to certain group of users. Other tools are used by a wider audience with a wider range of interests.

When reviewing different circumvention tools we want to ask ourselves: Who are the typical users of certain tool? Will the usage of certain tool link their users to a certain organization or donor?

We assume that tools with a diverse set of users are more suitable for circumvention as they can not bind a user to a certain group of people or organization.

In our review we were looking for tools that are used by a wider audience of users.

### **7.4.2 Logging practises**

What information is stored in the proxy that is handling the users request? Are IP address and URLs logged? Where are the logs stored and for how long? What is the purpose of the logging? 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 our review we were looking for tools that know how to handle logging and inform correctly users about such practises.

### **7.4.3 End-user privacy**

An important aspect of a circumvention tools is the ability to hide where the initial request come from. Some tools like put great efforts into hiding the end users digital identity, while others do very little or nothing to hide this data. A good example of the importance of this type of privacy is the case of Yahoo<sup>4</sup> turning over information about one of its Chinese webmail users to the Chinese government. If Yahoo would not have such

---

<sup>4</sup> Read about the Wang Xiaoning case at [http://en.wikipedia.org/wiki/Wang\\_Xiaoning](http://en.wikipedia.org/wiki/Wang_Xiaoning)

type of information, they could not have given it away.

In our review we were looking for tools that have an end-user privacy policy.

#### **7.4.4 Location Privacy**

Location privacy is critical when using circumvention tools that can run from mobile devices or laptops connected to 3G mobile networks. Lack of location privacy implies that user preferences including favourite websites or software tools can be linked to several unique identifiers as the mobile subscriber and equipment identifier.

### **7.5 Infrastructure Development**

#### **7.5.1 Decentralized vs Centralized**

Proxy based circumvention tools route Internet traffic through one or more intermediaries (proxy servers) to retrieve the blocked content. These intermediaries can be either operated by the very same organization that develops the technology, or alternatively run by a third party individual or organization.

A great of trust is delegated to those organizations operating the proxy servers. Those who operate the intermediaries can always log all traffic passing through including source and destination IP addresses. In general, we can assume that the bigger the number of possible intermediaries the smaller the chances that all operators engaged in undesired logging practices. The bigger the choice the better!

Some tools increase the level of trust by securely routing the traffic through several intermediaries. In contrast with the technologies that use one single proxy, in a multi-hop proxy solution, the collaboration among all intermediaries at a given time is needed to track users IP addresses and their requests.

In our review we were looking for tools that use more than one intermediary.

#### **7.5.2 Resilient**

Although a few tools start to consider peer-to-peer models, the majority of the solutions rely heavily in a client-server architecture where a specific piece of software interfaces with a server side infrastructure. The challenge that many solutions face is how to quickly adapt to traffic monitoring (deep packet inspection) and ultimately filtering and blocking.

Many solutions use dynamic intermediaries that are not fully disclosed to ensure that full

blocking is futile. Other solutions change the type of tunnels to try to mitigate certain kinds of blocking. In any case, tools need to learn from adversaries and have the capability and flexibility to adapt to new situations.

### **7.5.3 Speed**

The speed of a circumvention tool depends mainly of the amount of bandwidth available across the virtual channel created between the user and the final destination.

You can expect a slower response the bigger the number of intermediaries are used. Forcing the traffic to travel by an alternative path that can include locations spread all around the world has an impact in speed. Tools that proxy one single type of traffic (e.g. web traffic only) tend to perform better than those that allow any type of application. Tools open to any type of traffic are clogged by peer to peer (P2P) traffic and audio and video streaming, applications that are bandwidth hungry.

There is a clear trade off between speed and trust. Solutions that use one single intermediary perform better at the expense of less confidentiality.

In our review we were looking for infrastructure that can effectively provision bandwidth to the users.

## 8 Tools Evaluation

### 8.1 Dynaweb

#### Developers

Dynaweb was launched in 2002 by *Dynamic Internet Technology* (DIT) thanks to the support of the US 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*<sup>5</sup>, which is an alliance of organisations developing anti-censorship technologies. Most of the alliance members have Chinese background, mainly within Falun Gong.



After the 2009 uprising in Iran, Dynaweb is also providing access to Iranian users. Although DIT's CEO Bill Xia<sup>6</sup> is publicly known for his advocacy against the Chinese government, DIT's technology and its internal expertise is impossible to evaluate from an outsider. DIT does not seem to follow the traditional open design best practices and claims like that their software constantly circumvents the Chinese *Golden Shield Project* are not scientifically justified.

The fact that end users can not verify their developers' expertise in the field of network security and privacy, nor audit the source code of the tools, gives their tools a very low level of trustworthiness.

The history of DIT has raised plenty of eye brows. In several occasions Dynamic Internet Technology's tools have been labeled as a virus or a trojan by popular anti-viruses<sup>7</sup> and in early 2009, a web posting<sup>8</sup> about Dynaweb potential use of personal data, triggered an open discussion about the privacy policy of the project.

#### Technology

Dynaweb is a web based proxy service. The tool uses a limited pool of proxy servers, most

<sup>5</sup> Global Internet Freedom Consortium <http://www.internetfreedom.org/>

<sup>6</sup> Bill Xia, a Chinese dissident (and Falun Gong practitioner) based in the US, that is devoted to fight the Internet censorship of China.

<sup>7</sup> Symantec Relabels Freegate [http://www.theregister.co.uk/2004/09/16/symantec\\_relabels\\_freegate/](http://www.theregister.co.uk/2004/09/16/symantec_relabels_freegate/)

<sup>8</sup> 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/>

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 and has looked into the Golden Shield Project<sup>9</sup>.

### **Disadvantages**

The pool of proxy servers Dynaweb is using are all equipped with uncertified SSL certificates which easily can be impersonated.

The URL that Dynaweb is providing to the users contains a fingerprint<sup>10</sup> that can be easily can be blocked by application layer firewall, for example:

[http://us.dongtaiwang.com/do/Qa\\_k/tttLwwxLx0LbC/](http://us.dongtaiwang.com/do/Qa_k/tttLwwxLx0LbC/)

Confidentiality of the web requests is guaranteed by means of HTTPS but unfortunately SSL certificates are bogus and impersonation of proxies is feasible. Users of Dynaweb are easily observable and and linkable to the technology. Not all content is reachable via Dynaweb and the proxies decides what content falls under their service policy.

## **8.2 Freegate**

### **Developers**

Freegate is another circumvention tool developed by DIT (See Dynaweb)

### **Technology**

Freegate installs two local proxies with SOCKSv5 support in ports 8580 and 8567. The local proxies 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 Freegate seems to use several domain names around the world, the IP space is limited to a few providers located in Taiwan and U.S.A.

No application layer special filters are provided that protect the user from Javascript, Java or Flash identification attacks.

<sup>9</sup> [http://en.wikipedia.org/wiki/Internet\\_censorship\\_in\\_the\\_People's\\_Republic\\_of\\_China](http://en.wikipedia.org/wiki/Internet_censorship_in_the_People's_Republic_of_China) (Accessed April 2010)

<sup>10</sup> All URLs contains the fingerprint “ tttL”



**D·I·T**  
DYNAMIC INTERNET TECHNOLOGY

Tool: Freegate  
Developers: Dynamic Internet Technology (DIT)  
Website: [www.dit-inc.us](http://www.dit-inc.us)  
Technology: Local proxy (SOCKSv5)  
Grade: 1

Theoretically, since January 2009 the tool is only available for Chinese and Iranian users. During our testing we could bypass this geographical location limitation.

### Advantage

Simple to use, a downloadable client without installer. Can be run as portable application.

### Disadvantage

Just like Dynaweb, there is no 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.

It is difficult to verify the integrity of the software and if includes any back-doors or spyware.

## 8.3 GTunnel


### Developers

Gtunnel is developed by *Garden Networks for Information Freedom*<sup>11</sup>, a non-profit organization based in Canada. Since 2001, the organization had provided anti-censorship software to Chinese Internet users.

### Technology

GTunnel is a 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 Register and setting a local proxy in port 8081. As many other tools from the *Global Internet Freedom Consortium* the proxy 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 offers the possibility to channel the traffic through the Skype<sup>12</sup> or the Tor network. which makes tool a high rank in terms of availability. The software also claims that the traffic could channeled through Gtalk but we were not able to verify this functionality.



Tool: Gtunnel  
Developers: Garden Networks for Information Freedom  
Website: [www.gardennetworks.org](http://www.gardennetworks.org)  
Technology: Local proxy (HTTP/SOCKS)  
Grade: 1

<sup>11</sup> Website: [www.gardennetworks.org](http://www.gardennetworks.org)

<sup>12</sup> In our tests, we needed to use an old version of Skype (3.6)

One interesting aspect of the technology is the novel use the Skype network as a transport layer as in theory should provide better levels of unobservability while maintaining the confidentiality in the data traffic.

### **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 to other peers through firewalls. In countries where Skype is blocked,

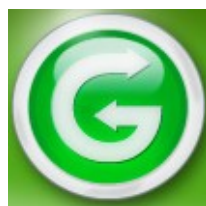
### **Disadvantage**

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.

## **8.4 Gpass**

### **Developers**

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



Tool: GPass

Developers: *Word's Gate Inc*

Website:

<http://gpass1.com/gpass>

Technology: Multi-featured tunneling service

Grade: 3

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

### **Technology**

Although GPass claims to be a different tool than Gtunnel, both tools seem to share the core technology and GPass looks like 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. Unfortunately Gpass provides no more substantial new features than Gtunnel and there is real encrypted storage or personal data management included in the tool. GPass is a downloadable client, that needs to be installed on the users computer.

## Advantages

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

## Disadvantage

The software has not been audited. As for any other circumvention tool based on a downloadable client, it can be a hassle for the user to get hold of the software, since the site distributing the software often is blocked.

Since the software needs to be installed, it can not be used as a portable application. Also, it is not possible to hide its existence once it has been installed.

## 8.5 Google (reader, translation, cache)

### Developers

Not surprisingly, Google Inc. is the company behind 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 fetch blocked content. To find the pointer to the cached content, the user needs to reach the Google search engine first (so Google can not be blocked). 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*<sup>13</sup>. Using Google cache does neither hide your IP, nor the data being transferred (no HTTPS support).

*Google Reader:* Google offers users the possibility to subscribe to news feeds through Google Reader which fetches the data on the users behalf (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 of course that Gmail is not blocked. The user is limited to access content that is stored in RSS feed header. To read the full RSS entry, the user needs to be



Tool: Google  
Developers: Google Inc.  
Website: [www.google.com](http://www.google.com)  
Technology: Website cache, translation service etc.  
Grade: 4

<sup>13</sup> <http://opennet.net/bulletins/006/>

able to reach the source website directly.

*Google Translate:* Google's translation service can be used to fetch blocked content. By setting the source language to something different what it is, and setting the target language to the actual source language, Google Translate will fetch the request data and leave it non-translated. Google Translate does not provide HTTPS. Hence, your web request can be read in plain text on the wire.

### **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 public computers.

### **Disadvantage**

These free services are not developed with anonymity and privacy in mind, and they are therefore not providing a secure service suitable for users in countries where heavy monitoring is taken place.

## **8.6 Hotspot shield**

### **Developers**

Hotspot Shield is a software developed by AnchorFree, which is a private US based company that was founded in early 2005 by David Gorodyansky and Eugene Malobrodsky.

The thriving force behind the software was (no more no less that) to put users in control of their Internet activities, and to provide user privacy on the Internet. The target audience are common people in the Western world doing online shopping, and using insecure WiFi networks, not users in blocked countries.

The business model of the free software is sponsored personalized ads.

### **Technology**

Hotspot Shield offers a VPN (virtual private network) between the client and their gateway. The software secures web sessions by HTTPS and hides the user's IP address. The software is available for Windows and Mac OS.

Tool: Hotspot Shield	
Developers: AnchorFree	
Website: <a href="http://www.anchorfree.com">www.anchorfree.com</a>	
Technology: VPN	
Grade: 1	

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](http://www.rss2search.com) a RSS feeds based search engine.

The search portal is full of ads, and gives the software a rather messy and unprofessional touch. The user can either use one of the provided search engines (that are not obvious to find) or type in a correct URL into the browser address window. An attempt to visit [Google.com](http://Google.com) 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 hits <sup>14</sup> 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 winter Olympic games).

Each page visited by Hotspot shield has a banner the contains the Hotspot Shield logo and a commercial ad. The ad can be removed from the web page by ticking a checkbox (on each and every page you visit), but the software logo remains (and is not very discrete!).

## **Advantage**

Hotspot Shield is a free VPN service that encrypts the tunnels the traffic from the user to one of the Hotspot gateways. It is reported that their publicly known gateways remain unblocked in China<sup>15</sup>.

## **Disadvantage**

After un-installing 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.

One does not need to be a genius to understand that personalized advertisements in an anonymizer tool is not a perfect match. It might work for a student circumventing the University blockage to access P2P, but not for a Burmese activist in Rangoon.

---

<sup>14</sup> A Google search on the same string gives 2,550,000 hits

<sup>15</sup> How To Search Google Uncensored In China

<http://www.businessinsider.com/hotspot-lets-youcheck-google-in-china-2010-3>

## 8.7 JAP

### Developers

JAP is an open source Java based client program used to access the JonDonym anonymization service. JonDonym is the commercial development face of 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)<sup>16</sup>, 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 US, the Netherlands, Denmark, the Czech republic and Switzerland.


The technology does not only provide *anonymization* (of your identity) and confidentiality (no one can read the content being sent) on the Internet, it also ensures *unobservability*, since no single proxy server can identify you and follow your Internet activities.

In order to support many applications, as 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 PortableApps), which makes it an excellent client for Cyber Café users. The trustworthiness of the software is very high due to the reputation of the developers (researchers from well respected University), and the openness of the code (source code available in CVS). The team behind the software is also open about *theoretical threats*<sup>17</sup> to the software, that the technology can not provide protection against.

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

Tool: JAP	
Developers: AN.ON research project, Dresden University of Technology (Germany), University of Regensburg (Germany)	
Website: <a href="http://anon.inf.tu-dresden.de">http://anon.inf.tu-dresden.de</a>	
Technology: Anonymous proxy server	
Grade: 7	

<sup>16</sup> 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.

<sup>17</sup> 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.

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 still carries the image of a research project. In the past JAP has been target of police investigation and criminalized and the project needs to be implement the European legal requirements of data retention<sup>18</sup>. Documentation<sup>19</sup> and localized GUI<sup>20</sup> is only available in English and German. The number of mixes and Mix Cascades are limited, only 6 of them are available for free. This raises the question how well the technology scales up for non-premium users, and how easy the existing mixers can be blocked. However, it is possible for “anyone<sup>21</sup>” to set up a mixer server to serve a community of users with the JonDonym technology.

## **8.8 Psiphon**

### **Developers**

Psiphon is developed by the Citizen Lab, Munk Centre for International Studies, at the University of Toronto, Canada. There are two branches of Psiphon available, one open source version and one commercial version with add-on features. This review focuses on the open source version, which is released under GNU General Public License (GPL).

Psiphon (open source) was initially funded by the Open Society Institute. Since the spin off from the University in 2008, Psiphon is now established as a Canadian corporation and has received additional funding from a number of government based donors mainly from US, UK and the EU.


Tool: Psiphon
Developers: Citizen Lab, Munk Centre for International Studies, University of Toronto, Canada.
Website: <a href="http://psiphon.ca">http://psiphon.ca</a>
Technology: Web proxy (HTTPS)
Grade: 8

### **Technology**

Psiphon is a web proxy that uses the HTTPS protocol to transfer data securely between

<sup>18</sup> Implementation of data retention according to the German Telecommunications Act [http://anon.inf.tu-dresden.de/dataretention\\_en.html](http://anon.inf.tu-dresden.de/dataretention_en.html)

<sup>19</sup> Documentation is mainly available in English and German.

<sup>20</sup> The installer and the GUI is localized to German, Czech, Dutch, French and Russian

<sup>21</sup> Anyone with the right technical capacity and financial means

the user and the proxy server. Psiphon provides privacy, but not full anonymity, since the proxy server logs all client activity.

The uniqueness of Psiphon is that the solution relays in a decentralized model where people with connections in the “unblocked” parts of the world can assist individuals suffering Internet blocking. For Psiphon to work, users need to find one trusted partner in a non-blocked country that can channel the traffic for them.

### **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 traces on the users computer, as long as the browsing history is erased. This approach makes Psiphon an excellent portable application which can be used from Cyber Cafés.

Documentation is available in five languages, and is excellent in terms of content, pedagogic and illustrations.

### **Disadvantage**

Although the “trust model” is an excellent solution to the problem with untrusted public proxies, it can also be a bottleneck, as not everyone in a blocked country knows someone in a non-blocked country and has the skills to set up a Psiphon node. Hence, the accessibility of Psiphon is presumable quite low in comparison with other proxies that are open for the public.

### **Comment**

The software has a high trust level, based on open-source software, public development team, connection to respected Universities, and the focus on users in blocked countries, rather than P2P thirsty students behind a University firewall.

## **8.9 Tor**

### **Developers**

The Tor Project is since December 2006 a 501(c)(3) non-profit based in the United States (Dedham, MA). Tor is the latest implementation of the Onion Routing system, a information hiding design published and deployed in the mid 1996. 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

Tool: Tor

Developers: Tor Project, a US based non-profit.

Website: [www.torproject.org](http://www.torproject.org)

Technology: onion routing/telescopic encryption

Grade: 9



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 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 a publicly available source code and protocol specification.

## **Technology**

The Tor project main goal is to develop a network that projects the privacy of TCP connections. Tor basic principle is to bounce the 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 shared secrets of the exit node, intermediary and entry node.

Tor was not originally designed as a circumvention tool rather a mechanism to resist traffic analysis attacks. But as Tor channels the traffic via a virtual circuit, it allows to circumvent Internet blocking. The common method to block Tor is restrict the access to the seven directory (authoritative) servers to have a view the network<sup>22</sup>. To strength the resistance against this kind of attacks, Tor developers have extend their protocol to encrypt directory lookups and to allow users to use intermediaries not published in the directory to relay the traffic. This new intermediaries are known as “Tor bridges” and their IP addresses can be retrieved by alternatives means (mail requests, internet messengering, etc)<sup>23</sup>.

Tor project also aims to provide basic application level anonymity by including a proxy that filters personal data in web requests from 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 do and what it can't. Their

---

<sup>22</sup> Blocking Tor servers <http://blog.vorant.com/2008/06/tor-server-lists-revisited.html>

<sup>23</sup> Tor partially blocked in China <https://blog.torproject.org/blog/tor-partially-blocked-china>

infrastructure is highly distributed and with the bundle of tools in one single installer, the technology is accessible to normal users.


## **Disadvantage**

Tor Developers are aware of the current limitations of Tor<sup>24</sup> and the overall perception that the Tor network is slow. Tor does not behave well in highly congested Internet connections, and although efforts are documented to improve Tor behaviour<sup>25</sup> non very technical users 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 the average users to trade speed for privacy.

## **8.10 Ultrasurf**

### **Developers**

Ultrasurf is another product from the Global Internet Freedom Consortium, this time developed by UltraReach, a group of entrepreneurs based in US, but with roots in China. The team of developers behind the tool is not public, and very little information

Tool: UltraSurf	
Developers: UltraReach	
Website: <a href="http://www.ultrareach.com">http://www.ultrareach.com</a>	
Technology: HTTP proxy	
Grade: 3	

about UltraReach is available on their website. The main focus of Ultrasurf is circumvention in China.

### **Technology**

UltraSurf uses HTTP proxying to allow users to access blocked content. Very technical details are available in the website apart from mentioning several buzzwords and that is based on a technology called GIFT (Global Internet Freedom Technology) that happens to be the same technology that the UltraReach team develops. 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 favourite browser (IE or Firefox).

### **Advantage**

<sup>24</sup> Why tor is slow? <https://blog.torproject.org/blog/why-tor-is-slow>

<sup>25</sup> Improving Tor speed <https://trac.torproject.org/projects/tor/wiki/TheOnionRouter/FireFoxTorPerf>

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 or 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 odd behaviour on computers with Ultrasurf installed has been documented, there has not been a clear and proven case against the tool. What is odd though, is that the only reaction from Ultrasurf has been to simply deny the accusations, instead of proving more evidence of their innocence. On the UltraSurf website, the following statement can be read:

*“UltraSurf provides users with state-of-the-art internet technology to break through firewall safely. It is a popular anti-censorship software, not a Trojan or virus.”*

*“Please rest assured that UltraSurf will not touch any of the documents on your PC.”*

The best way to handle the accusations would be to (1) publish the code for public review, or (2) invite a trustworthy institution for an audit.

## **8.11 Your Freedom**

### **Developers**

Your Freedom is developed by the private business *re:solution - Reichert Network Solutions GmbH*, Germany, 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 is restricted in terms of bandwidth and number of simultaneous streams.

### **Technology**

Your Freedom is a proxy tunneling software (HTTP and SOCKS) with support for HTTPS, FTP and UDP services. The software allows web browsers, chat services and file sharing applications to access their network of proxies<sup>26</sup>. The software is Java based, and is available for Windows, Linux and Mac OS.



**WWW.YOUR-FREEDOM.NET**  
OPENS YOUR DOOR TO THE WORLD

Tool: Your Freedom

Developers: re:solution - Reichert Network Solutions GmbH, Germany

Website: [www.your-freedom.net](http://www.your-freedom.net)

Technology: Proxy tunneling software (HTTP/SOCKS) with support for HTTPS, FTP and UDP services.

Grade: 6

<sup>26</sup> The network consists of 18 proxies located in 3 countries. [April 2010]

The developer highlight that Your Freedom is *not* a perfect anonymizer since the software can not protect the user from him or her own mistakes and existing flaws in applications and protocols (that might reveal your real IP address). Your Freedom hides your IP address unless an application you are using carries it "inband" (for example in HTTP headers) .

### **Advantage**

The software is simple to use although it provides privacy and anonymity with sophisticated methods. The documentation (50+ pages User Guide) is an excellent resource to learn the tool and understand the underlying technology. The guide explains what protection the tool provides, and what it 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 Relays<sup>27</sup> to support the limiting number of proxy servers.

### **Disadvantage**

The main target group of the tool is common people that for one reason or another is sitting behind a firewall (students at a University, employees at a corporation). Therefore, the tools is designed to get around circumvention, with little focus on hiding the existence of the tool<sup>28</sup> or providing a clean un-installation<sup>29</sup>, portability<sup>30</sup> and easy access to the tool<sup>31</sup>.

## **9 Our testing laboratory**

It is not the goal of this report to provide a comprehensive document of how to mirror our test environment. We understand the sensibility of some of our results and decided not to public any information that could be used and abused by the lazy readers. Nevertheless we understand that the technical reader might be interested to know how deep we have looked into the tools.

Our testbed consisted in two Linux boxes running Ubuntu 8.04 LTS and Virtualbox virtualization software. A copy of Windows XP was installed as guest operative system of Virtualbox. During the month of March 2010, each of the tools was tested individually in

---

<sup>27</sup> CGI Relays <http://www.your-freedom.net/index.php?id=156>

<sup>28</sup> The tool needs to be locally installed on the computer.

<sup>29</sup> Using the un-install feature leaves several Windows registry entries containing the name "Your Freedom"

<sup>30</sup> The tool can not be run portable.

<sup>31</sup> The user needs to register online, activate her account (by email invitation), to download the software.

an independent instance of Windows XP with the latest software update and service packs.

In order to monitor what changes each tool performed in the operative system, we used two powerful tools from Microsoft Sysinternals: Process Monitor<sup>32</sup> and TCPView<sup>33</sup>. As Windows is running as guest operative system of Linux in a virtualized environment, we were able to double check the results offered by TCPView by using the popular Linux packet sniffer Wireshark.

Using Linux kernel firewall utilities (iptables) and proxy servers (squid) we simulated the most common attacks against the circumvention technologies including DNS poisoning and selective UDP and TCP port blocking. Using IP geolocation tools as BGP looking glasses in five major Internet exchanges we were able to triangulate and locate the hosting location of major proxy services.

In order to generate lists of proxy's IP addresses, random email addresses were generated to perform queries against mail robots. Yes, we basically mail the robots from different locations and e-mail addresses. To evaluate the performance of different tools from different countries we tunneled our traffic using OpenVPN. In order to simulate network congestion and packet loss Dummynet<sup>34</sup> was used.

Our tests were performed during a very limited time (two weeks). We are aware that the network situation changes rapidly in countries under complex political circumstances and understanding blocking practises requires further resources and ongoing sampling of data.

## 10 Recommendations

1. Sustainability of circumvention solutions can only be achieved by suitable business models to cover the costs of continuous research and development, infrastructure and dissemination. There is no solution that can survive as a result of one-time investment.
2. Sustainability of circumventions solutions can not rely in one single country or environment. Tools need to be built with flexibility in mind.
3. Trust requires the peer review of the technologies and technical implementations involved in the solutions.
4. Trust requires to be open about the limitations of the solutions provided and to properly inform their users about the risk that they assume when using the tools.
5. Usable solutions are not only those that perform functional tasks but are able to educate the user about the choices is making.

---

<sup>32</sup> <http://technet.microsoft.com/en-us/sysinternals/bb896645.aspx>

<sup>33</sup> <http://technet.microsoft.com/en-us/sysinternals/bb897437.aspx>

<sup>34</sup> <http://info.iet.unipi.it/~luigi/dummynet/>

6. Usable solutions are those that have training materials and community support forums adequate to different target audiences.
7. Privacy regarding the use of the technology is a technical challenge that deserves further investment. Circumvention tools need to look into the technical mechanisms to conceal the fact that circumvention technology is in use.
8. Privacy and circumvention tools not necessary go hand in hand. Users have the right to be informed about what personal identifiable information is provided to the operator of the circumvention technology infrastructure.
9. Infrastructure development should be as distributed as possible taking advantage of the state-of-the-art of peer-to-peer technologies.
10. Infrastructure development needs to be combined with the incubation of communities of practitioners that can ultimately provide peer-to-peer localized support.

## 11 Tools Comparison Matrix

### Digested view of the results

	Dynaweb	Freerate	Gtunnel	Gpass	Hotspot	JAP	Phsiphon	Tor	Ultrasurf	Your Freedom	Google	AVG
S	0	0	0	0	0	1	1	2	0	1	2	3.18
T	0	0	0	0	0	2	2	2	0	1	0	3.18
U	1	1	1	2	1	1	2	1	2	2	1	6.82
P	0	0	0	1	0	2	1	2	1	1	0	3.64
ID	0	0	0	0	0	1	2	2	0	1	1	3.18
T	1	1	1	3	1	7	8	9	3	6	4	

