HANDBOOK FOR **BLOGGERS** AND **CYBER-DISSIDENTS**

REPORTERS WITHOUT BORDERS

MARCH 2008

REPORTERS
WITHOUT BORDERS
FOR PRESS FREEDOM

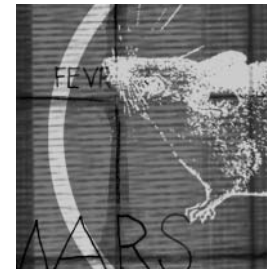
HANDBOOK
FOR BLOGGERS
AND
CYBER-DISSIDENTS

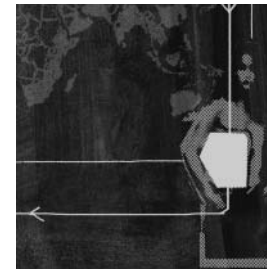
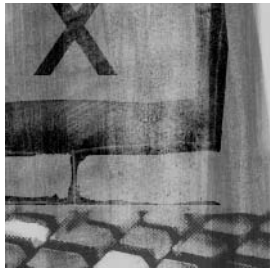
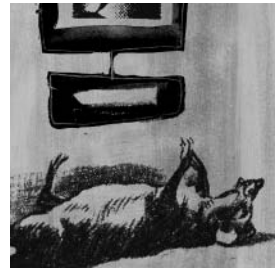
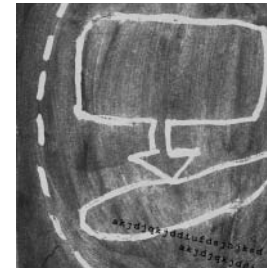
REPORTERS WITHOUT BORDERS

REPORTERS
WITHOUT BORDERS
FOR PRESS FREEDOM

HANDBOOK
FOR BLOGGERS
AND
CYBER-DISSIDENTS
CONTENTS





mine

BLOGGERS, A NEW SOURCE OF NEWS

By Clothilde Le Coz

Bloggers cause anxiety. Governments are wary of these men and women, who are posting news, without being professional journalists. Worse, bloggers sometimes raise sensitive issues which the media, now known as "traditional", do not dare cover. Blogs have in some countries become a source of news in their own right.

Nearly 120,000 blogs are created every day. Certainly the blogosphere is not just adorned by gems of courage and truth. It is also often the source of confusion and disinformation and not all bloggers have the souls of reporters. That is why this handbook contains advice on creating and updating a blog, with no other ambition than that of free expression. For others it will be a struggle to draw attention to a particular issue. The first concern therefore is to make a publication visible (see the Jotman article). This handbook also suggests ploys to get your blog well referenced online (see the Olivier Andrieu article) as well as "editorial" recommendations (Get your blog to stand out, by Mark Glazer).

Let's acknowledge that blogs are a fantastic tool for freedom of expression. They have unloosed the tongues of ordinary citizens. People who were until now only consumers of news have become players in a new form of journalism, a "grassroots" journalism, as expressed by Dan Gillmor (Grassroots journalism – see the chapter What ethics should bloggers have?), that is "by the people for the people".

Blogs are more or less controllable for those who want to keep them under surveillance. Governments that are most up to do date with new technology use the most sophisticated filtering or blocking techniques, preventing them from appearing on the Web at all. But bloggers don't just sit back and let it happen. The essential question becomes how to blog in complete safety. With a normal IP address, a blogger can be tracked down and arrested. Anonymity allows them to keep their freedom (See "How to blog anonymously).

In countries where censorship holds sway, blogs are sometimes the only source of news. During the events in Burma in the autumn of 2007, pitting monks and the people against the military junta, bloggers were the main source of news for foreign jour-

nalists. Their video footage made it possible to gauge the scale of the protests and what demonstrators' demands were. For more than two months, marches were held in the streets, then a massive crackdown was launched against opponents that only the Burmese were able to show, so hard did it become for the few foreign journalists who managed to enter the country to get back out with their footage. And bloggers could not get the footage out without getting round online censorship imposed by the government. This handbook seeks to help every blogger to fill in the "black holes" In news. The second part is devoted to techniques which can thwart filtering technology (Choose your method to get round censorship by Nart Villeneuve). With a little good sense and persistence and above all finding the technique best suited to the situation, every blogger should be capable of shaking off censorship.

Clothilde Le Coz
Head of the Internet Freedom desk

WHAT'S A BLOG?

By LeMondedublog.com

A "BLOG" (OR "WEBLOG") IS A PERSONAL WEBSITE :

- containing mostly news ("posts").
- regularly updated.
- in the form of a diary (most recent posts at the top of the page), with most of the posts also arranged in categories.
- set up using a specially-designed interactive tool.
- usually created and run by a single person, sometimes anonymously.

A BLOG'S POSTS :

- are usually text (including external links), sometimes with pictures and, more and more often, sound and video.
- can be commented on by visitors.
- are archived on the blog and can been accessed there indefinitely.

SO A BLOG IS MUCH LIKE A "PERSONAL WEBPAGE, EXCEPT THAT IT :

- is easier to set up and maintain and so much more active and more frequently updated.
- encourages a more open and personal style and franker viewpoints.
- greatly encourages discussion with visitors and other bloggers.
- sets a standard worldwide format for blogs, involving similar methods (two or three-column layout, comments on posts and RSS (Really Simple Syndication) feed.

THE LANGUAGE OF BLOGGING

By Lemondedublog.com

BLOG
Short for Weblog. A website that contains written material, links or photos being posted all the time, usually by one individual, on a personal basis.

(TO) BLOG
Run a blog or post material on one.

BLOGGER
Person who runs a blog.

BLOGOSPHERE
All blogs, or the blogging community.

BLOGROLL
List of external links appearing on a blog, often links to other blogs and usually in a column on the homepage. Often amounts to a "sub-community" of bloggers who are friends.

BLOGWARE
Software used to run a blog.

COMMENT SPAM
Like e-mail spam. Robot "spambots" flood a blog with advertising in the form of bogus comments. A serious problem that requires bloggers and blog platforms to have tools to exclude some users or ban some addresses in comments.

CONTENT SYNDICATION
How a site's author or administrator makes all or part of its content available for posting on another website.

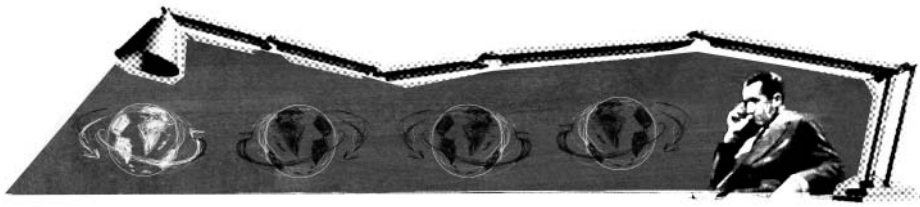
MOBLOG
Contraction of "mobile blog." A blog that can be updated remotely from anywhere, such as by phone or a digital assistant.

PERMALINK
Contraction of "permanent link." Web address of each item posted on a blog. A handy way of permanently bookmarking a post, even after it has been archived by the blog it originated from.

PHOTOBLOG
A blog mostly containing photos, posted constantly and chronologically.

PODCASTING
Contraction of "iPod" and "broadcasting." Posting audio and video material on a blog and its RSS feed, for digital players.

POST
An item posted on a blog. Can be a message or news, or just a photo or a link. Usually a short item, including external links, that visitors can comment on.



RSS (REALLY SIMPLE SYNDICATION)
A way of handling the latest items posted on a website, especially suited for blogs because it alerts users whenever their favourite blogs are updated. It can also "syndicate" content by allowing other websites (simply and automatically) to reproduce all or part of a site's content. Spreading fast, especially on media websites.

RSS AGGREGATOR
Software or online service allowing a blogger to read an RSS feed, especially the latest posts on his favourite blogs. Also called a reader, or feedreader.

RSS FEED
The file containing a blog's latest posts. It is read by an RSS aggregator/reader and shows at once when a blog has been updated.

TRACKBACK
A way that websites can communicate automatically by alerting each other that an item posted on a blog refers to a previous item.

WEB DIARY
A blog.

WIKI
From the Hawaiian word "wikiwiki" (quick). A website that can be easily and quickly updated by any visitor. The word has also come to mean the tools used to create a wiki (wiki engines). Blogs and wikis have some similarities but are quite different.

CHOOSING **THE BEST** TOOL

By Cyril Fi vet and Marc-Olivier Peyer and Lemondedublog.com

Blogs owe a lot to the growth of dynamic publishing tools that greatly simplify the business of updating websites.

A tool for use with a blog must provide a user-friendly interface (easily accessible through an Web navigator) and dynamically manage its content, with such things as archives and searches.

A blog has two Internet addresses that don't change after it's been set up:

- l'its address for public access.
- l'its administrative address, protected by a password belonging to the person who runs it.

You can set up a blog by either joining a blog community or using a blog tool with your own server.

BLOG COMMUNITIES

(See the chapter on "How to set up and run a blog: the Civiblog system")

Setting up a blog in an existing community usually takes just a few minutes. You pick a user-name and password and with a few clicks the blog is up and running. Some communities charge, some don't.

This method is best if you want to set up just a "view only" blog. It doesn't cost much (at most a few euros a month) and is straightforward and quick and you benefit from the traffic the community generates or from it being already well-known.

But snags include often limited options for layout and sophisticated features, as well as community-run ads and the risk of the community closing.

USING BLOG TOOLS

These are programmes that are installed on a server, using scripts to run the site automatically and a database to store posted material. Once installed, it operates through a standard online navigator. No special expertise, such as using HTML, is needed to set up and run a blog, but installing and configuring it is sometimes tricky (setting access criteria, creating a database and arranging FTP loading).

This solution is for people already familiar with blogs and has the advantage that it entirely belongs to you and you can therefore adapt, configure and alter it whenever you want. But it does requite some technical skill, is also more exposed (to spam comments) and you have to store the contents yourself.

HOW TO CHOOSE A BLOG COMMUNITY ?

It's not always easy to move from one blog community to another, so it's important to make a good choice in the first place.

Before choosing one, consider these points:

OTHER BLOGS IN A COMMUNITY

Some communities group Internet users according to interests or age. Have a look at several dozen other blogs in a community to see if it has a "typical" group.

WHAT THE BLOG LOOKS LIKE

Though the choice is often small, communities (platforms) usually have a fair range of colours, fonts and home-page layouts to choose from. You can get a good idea of the possibilities there too by looking at some of the community's sites at random. Many free-of-charge communities require all blogs to carry ads on all pages. Also check options for the blog's address, which could be http://myblog.thecommunity.com, http://www.thecommunity.com/myblog or http://www.thecommunity.com/mynumber.

FEATURES ON OFFER

Check these to see if you'll be able to redesign the blog, bring in other contributors, post images or sound, post things by phone or restrict access (totally or partially) to registered users. Also find out if posted material can be easily forwarded to another community and if you can insert paid ads to make money.

HIDDEN COSTS

Some communities are free but have to be paid for after a certain point, especially according to the amount of data stored and the bandwidth used. Check this beforehand.

INTERNATIONAL PLATFORMS

Blogger - http://www.blogger.com
Free.
Set up in 1999, bought by Google in 2003 and the biggest one of all, with eight million blogs. Easy to use but features rather limited.

LiveJournal - http://www.livejournal.com
Free or paid (about $2 a month).
One of the oldest platforms, with six million blogs, mostly young people.

MSN Spaces - http://www.msnspaces.com
Free.
Microsoft platform, set up in late 2004. Lots of features, some beyond the blog (photo-sharing, Messenger link). Must be aged at least 13 to register a blog.

FRENCH-LANGUAGE PLATFORMS

20six - http://www.20six.fr
Free or paid (ê 3-7 a month).
Lots of features, some quite sophisticated and including basic version.

Over-Blog - http://www.over-blog.com
Free.
Well-designed and easy to use.

Skyblog - http://www.skyblog.com
Free (with ads).
The biggest platform in France, very popular with young people, though features sometimes limited.

TypePad - http://www.typepad.com/sitefr
Paid (5-15 euros a month, according to number of features).
Very professional with good range of features.
A free version can be had through blog communities set up by third-parties, such as Noos (http://www.noosblog.fr) or Neuf Telecom (http://www.neufblog.com).

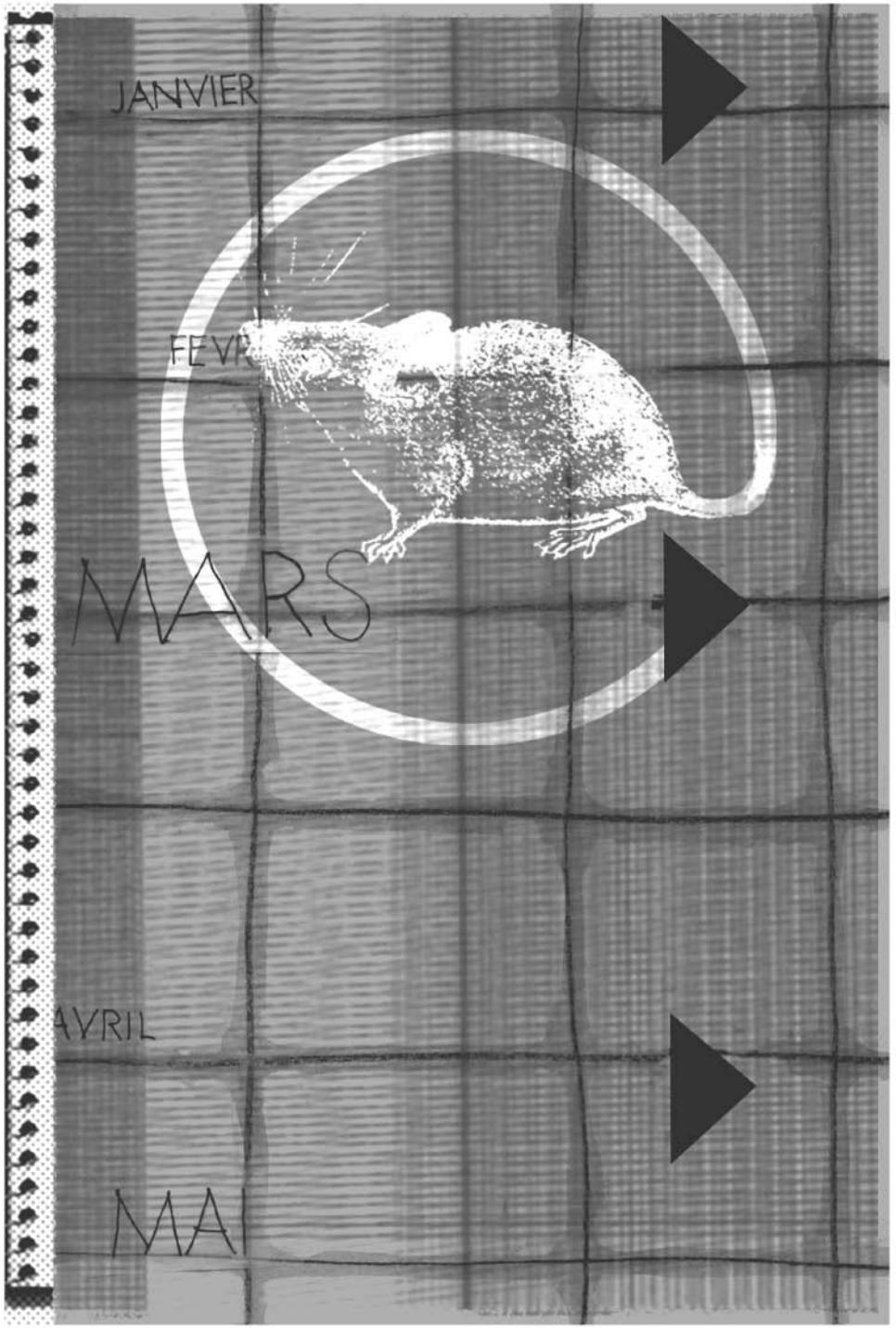
ViaBloga - http://viabloga.com
Free for non-profit associations, or 5 euros a month.
Original and dynamic, with some unusual features.

MAJOR BLOG TOOLS

DotClear - http://www.dotclear.net
MovableType - http://www.movabletype.org
Wordpress - http://www.wordpress.org

Lemondedublog.com is an daily update about the world of blogs and blogging

My blog


JANVIER
FEVR
MARS
AVRIL
MAI

HOW **TO SET UP AND RUN** A BLOG

The Wordpress system (www.wordpress.org)

Wordpress is very simple to use but requires to download a software to access the blog platform (it's a "blogware"). Wordpress is an "Opensource" project, which means that everyone can improve it through comments or suggestions.

It is however necessary to gather information on Wordpress security and privacy settings if you want to blog anonymously (cf."How to blog anonymously").

THE WORDPRESS HOMEPAGE

Wordpress is available in more than 120 languages (http://wordpress.com/languages/-). Each time you post an article, the platform is upadted through the RSS feeds.

SIGNING UP

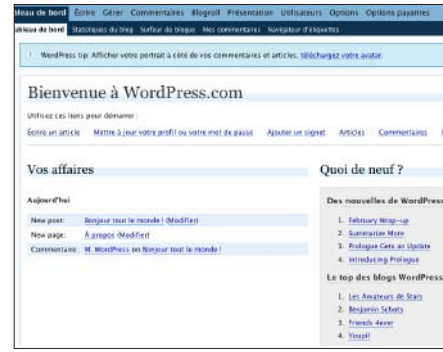
You have to register before you set up a blog. Most blog platforms make it very simple. Wordpress requires just basic details (login, password and e-mail address), and allows to blog anonymously. Access codes needed to launch the blog are e-mailed to the blogger.

ADMINISTRATION LOG-IN

A blog has a “front end” (the page where visitors go) and a “back end,” from where it’s updated, monitored and run and which is accessed with the user-name and password you get when you sign up.

DASHBOARD

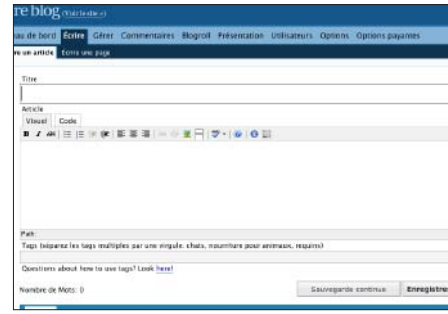
Most blogs have a "dashboard," where you can see at a glance everything happening on the blog, including the latest posts, comments and trackbacks. You can access all the blog's features from here and change how it looks, increase bandwidth, edit old posts and manage your users and their permissions, such as their right to post comments.



HOW TO POST

One of the big differences between a blog and a normal webpage is that it's easier to update a blog. Most platforms allow you to type posts in plain text without bothering about layout.

With Wordpress, you can change fonts, sizes and colours and insert links and pictures.



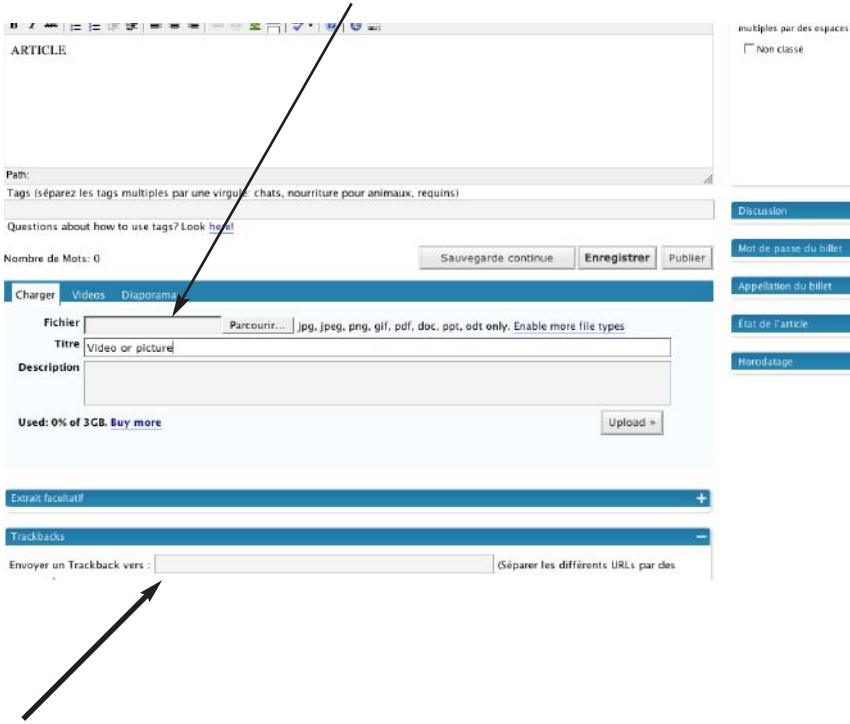
You post something by:

1. Logging in.
2. Clicking on "write."
3. Giving your post a name and typing the content in.
4. Formatting the text by using the interface.
5. Giving the post a category (so it can be grouped with similar ones) or creating a new category.
6. Clicking on "save" at the bottom of the page. Your article is in your "drafts"
7. click on "publish" to put it online. Be careful! If you want to blog anonymously, change the "timestamp" before publishing your post online. This way, you won't be related to this article if you post it from an controlled Internet cafe.

That's all. With a bit of experience, you can start using other features such as **"PINGS"**
A ping is a protocol that sends a message to another computer and waits for acknowledgment, often used to check if another computer on a network is reachable. They are essential to alert people on every update of your blog. But they can be dangerous to those who want to blog anonymously if they don't use a tool that can modify their IP address.

HOW TO PUBLISH A VIDEO

Publishing a video online makes your blog more attractiv.There are two ways of publishing a video. If you have the video file on your computer, you'll have to subscribe to the Wordpress paying version and use Wordpress video player. If the video is already online (on Youtube for example), click on "video" and add the link it is related to.



TRACKBACKS

It's easy to add a trackback to your post. You just add the permanent URL of the site you're referencing in the right-hand box marked "Sen a trackback to" and the trackback will automatically be sent to the site when you save the post.

LINK YOUR FAVOURITE WEBSITES TO YOUR BLOG
Click on "blogroll" and add the Internet addresses you want to be on your blog

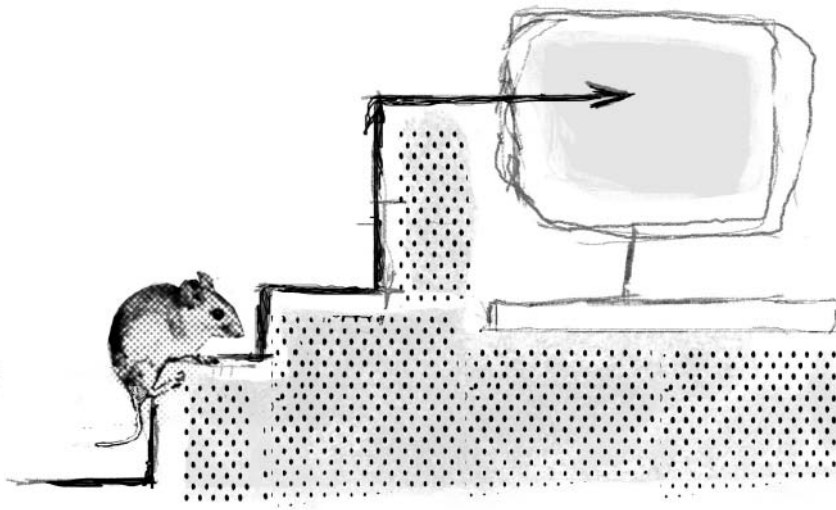
There are many websites about blogging. Here are some addresses :

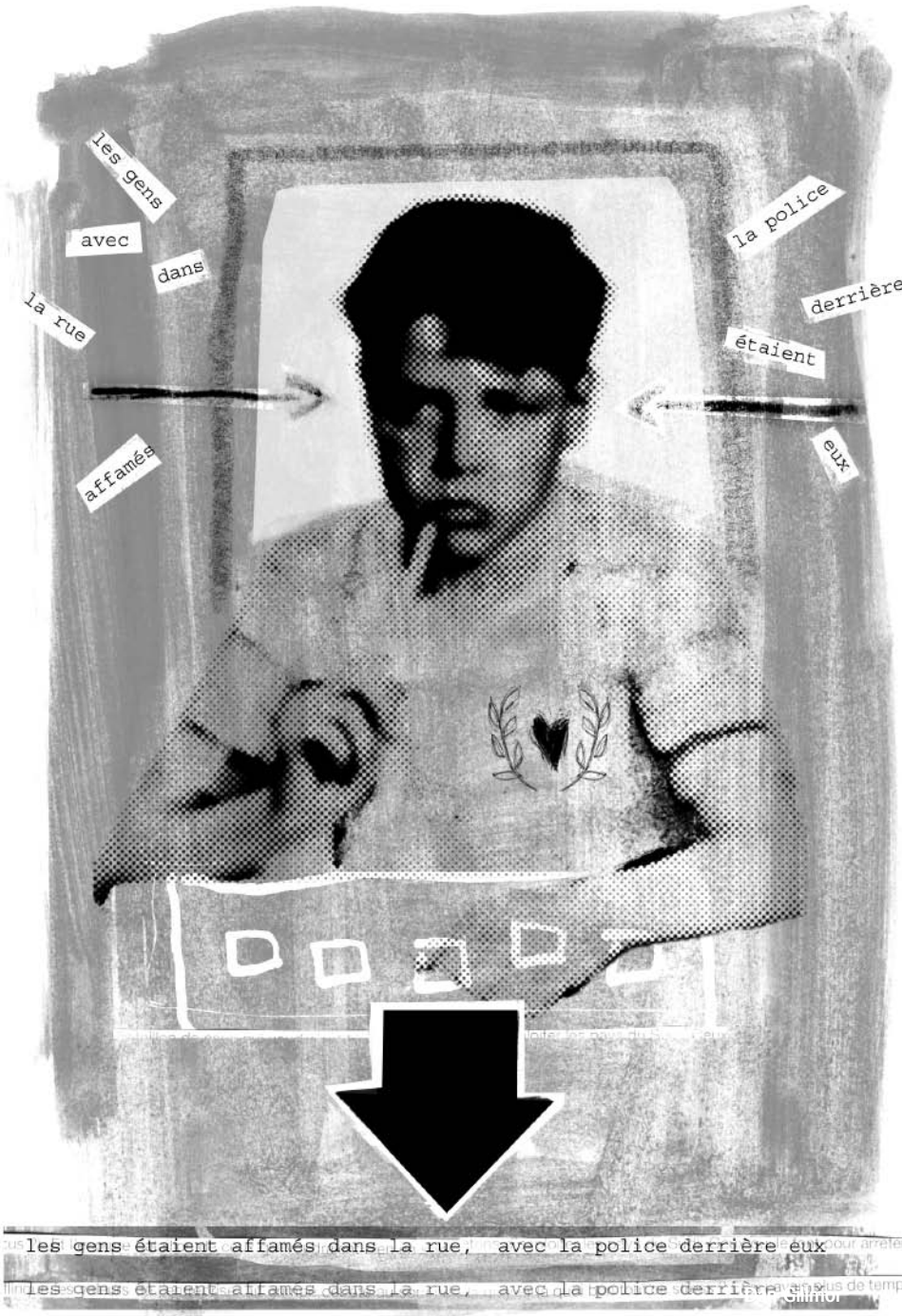
How to blog:
http://blogging.typepad.com/how_to_blog

The blogosphere:
http://blog.lib.umn.edu/blogosphere

The Weblog Workshop:
http://cyber.law.harvard.edu:8080/globalvoices/wiki/index.php/WeblogWorkshop

Blogging 101:
http://www.unc.edu/%7Ezuiker/blogging101/index.html





The people were hungry in the streets and the police were after them

WHAT ETHICS SHOULD BLOGGERS HAVE?

By Dan Gillmor

Not all bloggers do journalism. Most do not. But when they do, they should be ethical.

Does this mean they must subscribe to some kind of ethical code? Not necessarily.

The professional journalism world is awash in ethics codes. Some are longer than the United States Constitution, trying to anticipate every possible breach. Others are short and succinct, offering more positive guidance. The cyber-journalist Website has adapted for bloggers an ethics code (http://www.cyberjournalist.net/news/000215.php) from the Society of Professional Journalists, an American group. It is a solid and worthy effort.

All ethics codes are created for one essential purpose: to instill trust. If a reader (or viewer or listener) cannot trust the report, there is usually little reason to bother in the first place. The exception, of course, is looking at material that is known to be unethical, as much for instructional purposes – we can learn a great deal from watching unethical people's behavior – as to gain true knowledge.

For me, ethics is about something quite simple: honor. Within that word, however, is a great deal of territory. But unless we act with honor we cannot expect people's trust.

In American journalism, trust is often associated with a standard we call “objectivity” – the idea that an article should offer balance and nuance, giving the reader the chance to make up his or her own mind. I believe objectivity is a worthy but unattainable goal, because we all bring our own biases to everything we do.

In a world of new journalism, where we shift from a lecture to much more of a conversation, ethical journalism depends less on codes of ethics than the values and principles that are a foundation for honorable journalism.

There are pillars of good journalism: thoroughness, accuracy, fairness, transparency and independence.

The lines separating them are not always clear. They are open to wide interpretation, and are therefore loaded with nuance in themselves. But I think they are a useful way to approach ethical journalism, and they are notably easier to achieve in an online setting. Let's look at each.

THOROUGHNESS

When I was a reporter and, later, a columnist, my first goal was to learn as much as I could. After all, gathering facts and opinions is the foundation of reporting. I liked it best when I felt I had left 95 percent of what I'd learned out of the final piece. The best reporters I know always want to make one more call, check with one more source. (The last question I ask at all interviews is, “Who else should I talk with about this?”

Today, thoroughness means more than asking questions of the people in our address books, real or virtual. It means, whenever possible, asking our readers for their input, as I did when I wrote a book on grassroots journalism in 2004 (and as other authors are beginning to do in theirs). Competitive pressures tend to make this a rare request, but I'm convinced that more journalists will adopt it.

ACCURACY

Be factual.
Say what you don't know, not just what you do. (If the reader/listener/viewer does know what you don't, you've just invited him/her to fill you in.)
Accuracy means correcting what you get wrong, and doing it promptly. This is much easier online, where we can mitigate or at least limit the damage from our errors for new readers.

FAIRNESS

This one is as difficult, in practice, as accuracy is simple. Fairness is often in the eye of the beholder. But even here I think a few principles may universally apply.
Fairness means, among other things, listening to different viewpoints, and incorporating them into the journalism. It does not mean parroting lies or distortions to achieve that lazy equivalence that leads some journalists to get opposing quotes when the facts overwhelmingly support one side.
Fairness is also about letting people respond when they believe you are wrong, even if you do not agree. Again, this is much easier online than in a print publication, much less a broadcast.
Ultimately, fairness emerges from a state of mind. We should be aware of what drives us, and always be willing to listen to those who disagree. The first rule of having a conversation is to listen – and I know I learn more from people who think I'm wrong than from those who agree with me.

TRANSPARENCY

Disclosure is gaining currency as an addition to journalism. It's easier said than done, of course.

No one can plausibly argue with the idea that journalists need to disclose certain things, such as financial conflicts of interest. But to what extent? Should journalists of all kinds be expected to make their lives open books? How open?

Personal biases, even unconscious ones, affect the journalism as well. I'm an American, brought up in with certain beliefs that many folks in other lands (and some in the United States) flatly reject. I need to be aware of the things I take for granted, and periodically challenge some of them, as I do my work.

Another way to be transparent is how we present a story. We should link to source material as much as possible, bolstering what we tell people with close-to-the-ground facts and data. (Maybe this is part of accuracy or thoroughness, but it seems to fit here, too.)

INDEPENDENCE

Honorable journalism means following the story where it leads. When media are consolidated into a few big companies or are under the thumb of governments, this cannot happen.

It is simple to be independent online. Just start a blog. But no one should imagine that the same pressures from businesses and governments will not apply when a blogger tries to make a living at his or her new trade.

Jeff Jarvis, a prominent American blogger (buzzmachine.com), adds several other ideals. Bloggers must value the ethic of the conversation. He notes what for me is a bottom line of this new world: that conversation leads to understanding.

In a conversation, the first rule is to listen. Ethics requires listening, because it is how we learn.

Dan Gillmor is founder of Grassroots Media Inc., a company aimed at enabling grassroots journalism and expanding its reach. Its first site is Bayosphere.com in the San Francisco Bay Area. He is author of "We the Media: Grassroots Journalism by the People, for the People" (O'Reilly Media, 2004).

His blog:
http://bayosphere.com/blog/dangillmor

Elisabeth Fall, for O'Reilly Media

GETTING YOUR BLOG PICKED UP BY SEARCH-ENGINES

By Olivier Andrieu

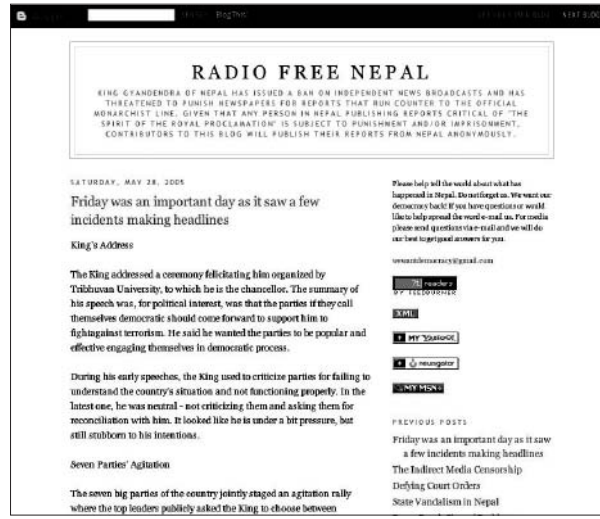
Blogs are websites themselves, so they're picked up by search-engines like Google, Yahoo! Search or MSN Search. To be successful, a blog has to get good visibility on their results pages through major keywords. So a site has to be designed from the start to react to the mechanical classification criteria these engines use.

Blogs have several built-in characteristics that get them often picked up by search-engines, well-listed and placed in a prominent position on results pages.

• Because they are personal diaries (at least at the beginning), they usually have a lot of text which helps them get picked up. Search-engines don't pick up sites with a lot of graphics or Flash animations but not much text.

• Each "post" usually occupies a single page, accessible through a "permalink" and dealing with a single subject, and is much more often picked up by search-engines than long pages about many different topics (such as archives or a blog homepage).

• The heading of a post is usually reproduced in the page heading or the URL (address). For example, on the Radio Free Nepal blog, at http://freenepal.blogspot.com, each post is on a page of its own, such as http://freenepal.blogspot.com/2005/04/state-vandalism-in-nepal.html:



RADIO FREE NEPAL

KING GYANENDRA OF NEPAL HAS ISSUED A BAN ON INDEPENDENT NEWS BROADCASTS AND HAS THREATENED TO PUNISH NEWSPAPERS FOR REPORTS THAT RUN COUNTER TO THE OFFICIAL MONARCHIST LINE. GIVEN THAT ANY PERSON IN NEPAL PUBLISHING REPORTS CRITICAL OF "THE SPIRIT OF THE ROYAL PROCLAMATION" IS SUBJECT TO PUNISHMENT AND/OR IMPRISONMENT, CONTRIBUTORS TO THIS BLOG WILL PUBLISH THEIR REPORTS FROM NEPAL ANONYMOUSLY.

SATURDAY, MAY 28, 2005

Friday was an important day as it saw a few incidents making headlines

King's Address

The King addressed a ceremony felicitating him organized by Tribhuvan University, to which he is the chancellor. The summary of his speech was, for political interest, was that the parties if they call themselves democratic should come forward to support him to fightagainst terrorism. He said he wanted the parties to be popular and effective engaging themselves in democratic process.

During his early speeches, the King used to criticize parties for failing to understand the country's situation and not functioning properly. In the latest one, he was neutral - not criticizing them and asking them for reconciliation with him. It looked like he is under a bit pressure, but still stubborn to his intentions.

Seven Parties' Agitation

The seven big parties of the country jointly staged an agitation rally where the top leaders publicly asked the King to choose between

Please help tell the world about what has happened in Nepal. Don't forget us. We want our democracy back! If you have questions or would like to help spread the word e-mail us. For media please send questions via e-mail and we will do our best to get good answers for you.

wewantdemocracy@gmail.com

readerz

XML

My Yahoo!

neuvigator

My MSN

PREVIOUS POSTS

Friday was an important day as it saw a few incidents making headlines

The Indirect Media Censorship

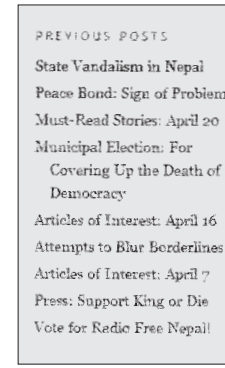
Defying Court Orders

State Vandalism in Nepal

The heading of the post (State Vandalism in Nepal) occurs not just in the page URL but also in the heading of the document, as follows :

So the post heading has been added after the blog's name, which appears alone on the blog's homepage (http://freenepal.blogspot.com).

The presence of descriptive keywords in the page headings (the content of the <TITLE> tag in HTML language) and in the URLs of these documents are key criteria for search-engines, so it's very important to choose post headings carefully to ensure they get picked up.



• Links are automatically created, especially to archives, and are text (see examples on the right of the Radio Free Nepal pages).

This is very good for getting picked up because the text content of the links (called "anchors") is key to the relevance of pages the links point to from the search-engines. So in the example here, the presence of the words "State Vandalism in Nepal" in the first link or "Radio Free Nepal" in the 9th boosts the relevance of the page indicated by the link for these terms. Also, the page with these links (the clickable text is detected as important by search-engines) and the page indicated by them will be considered relevant.

HOW TO GET A BLOG PICKED UP MORE

Blogs have many inbuilt advantages to get them picked up frequently. Once a search-engine has "found" the blog, either by it being submitted manually or by search-engine "spiders" following links, a blog will have much more chance than a standard website of being displayed prominently because of its natural advantages. But you should try to increase this visibility by going a bit further.

Here are some tips on how to do this, using major keywords drawn from the topic of your blog.

1. Focus on technology that helps getting picked up

If your site isn't yet online, be careful what technology (such as Blogger, Dotclear, BlogSpirit, Joueb and many others) you use to put it there. Choose the one that includes the maximum details for getting picked up:
• The heading of the post must be fully reproduced in the page heading (the <TITLE> tag) as well as in its URL (which isn't always done, since in the address some tools truncate the post heading after a certain number of characters).
• Creation of "permalinks" (links to a page containing a single post) must be possible.
• The technology chosen must allow you to do as much as possible in the design and personalisation of your site, such as using your own graphics and personal style-sheets. You must learn how to do as many technical things as possible so you can use the maximum number of factors to help the site get picked up.

To check all these points, have a look at sites using the technology you're considering (you can always find a big enough sample there) and see how they're displayed. You'll learn quite a lot this way.

2. Choose the best headings for your posts

This is very important. The heading of your post will be reproduced in the heading of the single pages displaying your posts, in their URLs and in the text of links that point to them – three key places for search-engines. So the post headings must contain, in a few words, the most important terms, to allow them to be picked up. Avoid headings such as "Well said!" "Welcome!" or "Great!" The heading should describe or sum up in less than five words what can be found in the post that follows. Think of the words you'd like a search-engine to pick up from it and put them in the heading. Not so easy, perhaps, but very effective.

3. Provide the text

Search-engines love text, so provide it for them. You can post all the photos you want as long as they go with text. Try to make each post at least 200 words long so it'll have a good chance of being easily spotted by search-engines. Also avoid having several very different topics in the same post, as search-engines don't like that. The golden rule is one topic, one post.

4. Pay attention to the first paragraph of your posts

The position of important words in the text is also crucial. Take great care with your first paragraph. If you want to be picked up with the words "release hostages," for example, put them among the first 50 in the post. The same goes for all the keywords you choose. A page with them at the beginning always gets better search-engine results than if they're at the end (all other things being equal). Stress these words, by putting them in bold for example. This signals to the search-engine that they're important.

5. Avoid duplicate content in a post

All search-engines have ways to detect duplicate content and if two pages are over-similar, only one of them will be spotted and the other rarely displayed on a results page. Google, for example, displays this message:
((In order to show you the most relevant results, we have omitted some entries very similar to those already displayed. If you like, you can repeat the search with the omitted results included.))

This often happens with blogs, as the pages containing each post can appear very similar.

For example, if you have an identical introduction on each page, either put it at the bottom or just on the home page, so as to make all your pages very different from each other.

6. Don't give your blog a title that's too long.

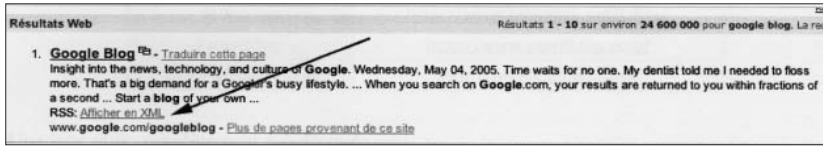
The best title (the content of the tag <TITLE>) for search-engines is between 5 and 10 words long, not counting "stop words" such as "the" or "and." The page heading of a blog usually has two parts:
• The general title of the blog
• A repeat of the heading of the post.

So as not to exceed 10 words in the general heading of pages presenting each post, you should use no more than five words for the general title of the blog and five for the heading of the post. That's not very much, but being concise as well as informative is one of the keys to getting picked up easily by search-engines.

If you can (not all technologies allow you to do it), put the heading of the post at the top and the general title of the blog afterwards, rather than the other way round.

7. Syndicate your blog

Most blog tools allow you to create an "XML thread" or "RSS feed" with which users can pick up your posts in suitable software format. You can offer this facility on your blog (it only takes a few minutes to install). You'll not only get more visitors but on Yahoo!, it'll be indicated prominently as shown: ((View as XML)).



So make use of this.

8. Keep your links updated

Links are very important for search-engines because they allow them to compile a popularity rating (called PageRank by Google) of webpages. So build up the number of links to your blog by:

- Inserting it in directories (see below).
- Looking for "cousin sites" that aren't rivals but offer material on the same topic. Exchanging links between blogs in the same area of interest should be sought as quickly as possible (this is quite frequently done and approved of in the blogging community, which is another advantage of blogs). Blogs are also well-suited for this, as the margin is often empty and they can be posted there.

FEATURING IN TOPIC DIRECTORIES

Featuring in general-interest search-engines (such as Google, MSN, Yahoo! and Exalead) and directories (such as Yahoo! Directory and Open Directory) is very important but getting featured by topic is too because it:

- generates more focused visitors.
- increases the number of links to your blog, which is good for your popularity.
- gets you known by other blog publishers who might want to exchange links with similar sites.

Among the many search tools (search-engines and directories) that pick up blogs, are:

English-language	Blogwise :	http://www.blogwise.com/
	Daypop :	http://www.daypop.com/
	Feedster :	http://www.feedster.com/
	Technorati :	http://www.technorati.com/
	Waypath :	http://www.waypath.com/
	Blogarama :	http://www.blogarama.com/
	Syndic8 :	http://www.syndic8.com/
French-language	Blogonautes	http://www.blogonautes.com/
	Blogolist	http://www.blogolist.com/
	Weblogues	http://www.weblogues.com/
	Blogarea	http://www.blogarea.net/Links/
	Pointblog	http://www.pointblog.com/
	Les Pages Joueb	http://pages.joueb.com/

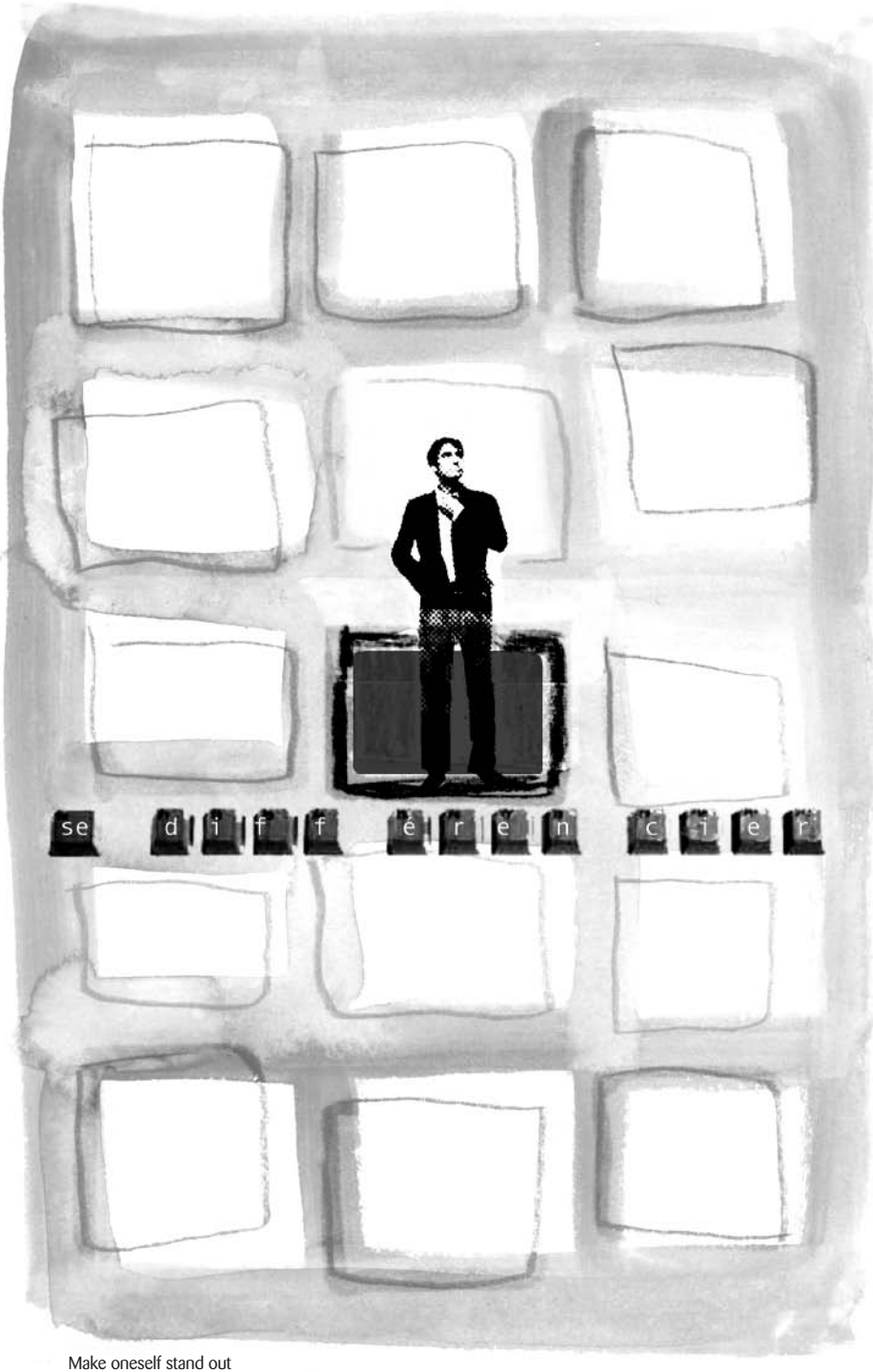
A bigger list is at :
http://search-engines.blogs.com/mon_weblog/2005/05/les_search-engines_de_.html

Also have a look at the directories of each technology provider, such as :
http://www.canalblog.com/cf/browseBlogs.cfm
http://www.dotclear.net/users.html
http://www.blogspirit.com/fr/communautes_blogspirit.html

CONCLUSION

A blog has all the elements for getting easily picked up by search-engines. With the tips given here, you should get very good results and increase your blog's visibility. So off you go – and remember that "content is king."

Olivier Andrieu is a freelance Internet consultant specialising in getting sites picked up by search-engines. He also runs the website www.abondance.com.



Make oneself stand out

WHAT REALLY MAKES **A BLOG SHINE**

By Mark Glaser

On the billions and billions of words posted by the millions of blogs worldwide, what makes one particular blog stand out from the teeming mass? What puts the blog writer into a special class, makes readers return day after day and brings accolades from the media?

It's connection. Successful bloggers are those who connect with their readers, whether 10 or 10,000 people, by entertaining or enlightening them. Many people like to draw boundaries between bloggers and other writers (journalists, novelists, marketers) but their goals are similar: grab people by the collar and don't let go.

Some of the bloggers writing in this handbook – Bahrain's Chan'ad Bahraini, Hong Kong's Yan Sham-Shackleton and Iran's Arash Sigarchi – blog in countries where the government is watching their words very carefully. And the world is watching them as well, to learn about stories the press in their countries dare not tell. In these places, freedom of speech and freedom of the press are in danger, and bloggers' voices online are an important link to the reality on the streets of their towns. The photos they take and the stories they tell are vital.

But what makes these and other noteworthy blogs shine? Here are some of their main attributes, the things that set them apart from all those millions of other blogs.

A UNIQUE AND PERSONAL VOICE

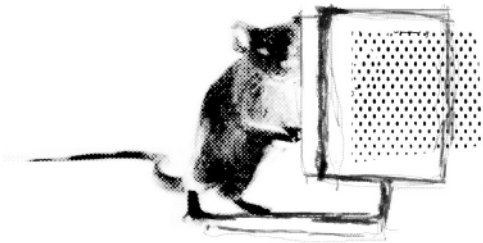
The best bloggers talk in their own voice, celebrate their unique identity and tell the stories that are real to them. Weblogs come from the idea of an online journal, a personal journal, so it's important to remember that journaling is not like academic writing, not like impersonal writing for a wire service. Chan'ad Bahraini is the pseudonym of an Asian blogger located in the mainly Arab country of Bahrain, giving him an unusual perspective on events there. Yan Sham-Shackleton is a performance artist who has lived all over the world and helped run a protest against China blocking the TypePad blog sites – after several years earlier herself helping the Chinese authorities to filter the Net.

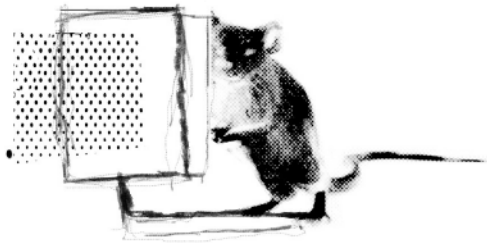
KEEP IT CURRENT

The biggest problem with the vast majority of blogs is that they are stale. Because most people are not paid to blog, it takes a while to integrate blogging into their daily routine. Many people start to blog, try it out, and then never have the time to update it. To be successful, bloggers must keep writing posts on a regular basis and stay up on the topics that interest them, including current affairs. That doesn't mean they have to post 12 times every day, but a few weeks off can kill a blog's audience.

CONNECT WITH AND EMPOWER READERS

One of the distinguishing features of blogs is interactivity. There are many ways to engage your readers, involve them in the conversation and utilize their feedback. You could run an online poll, or give them your e-mail address, or just enable comments under each posting. Jeff Ooi was threatened by the Malaysian authorities because of a comment made by one of his readers. Rather than take all comments off his blog, Ooi decided to moderate comments to make sure readers stayed on topic and would stand by their words. He also started up a Chinese-language blog called “The Ferryman” as a way to build a bridge between the Malaysian and Chinese blogospheres.

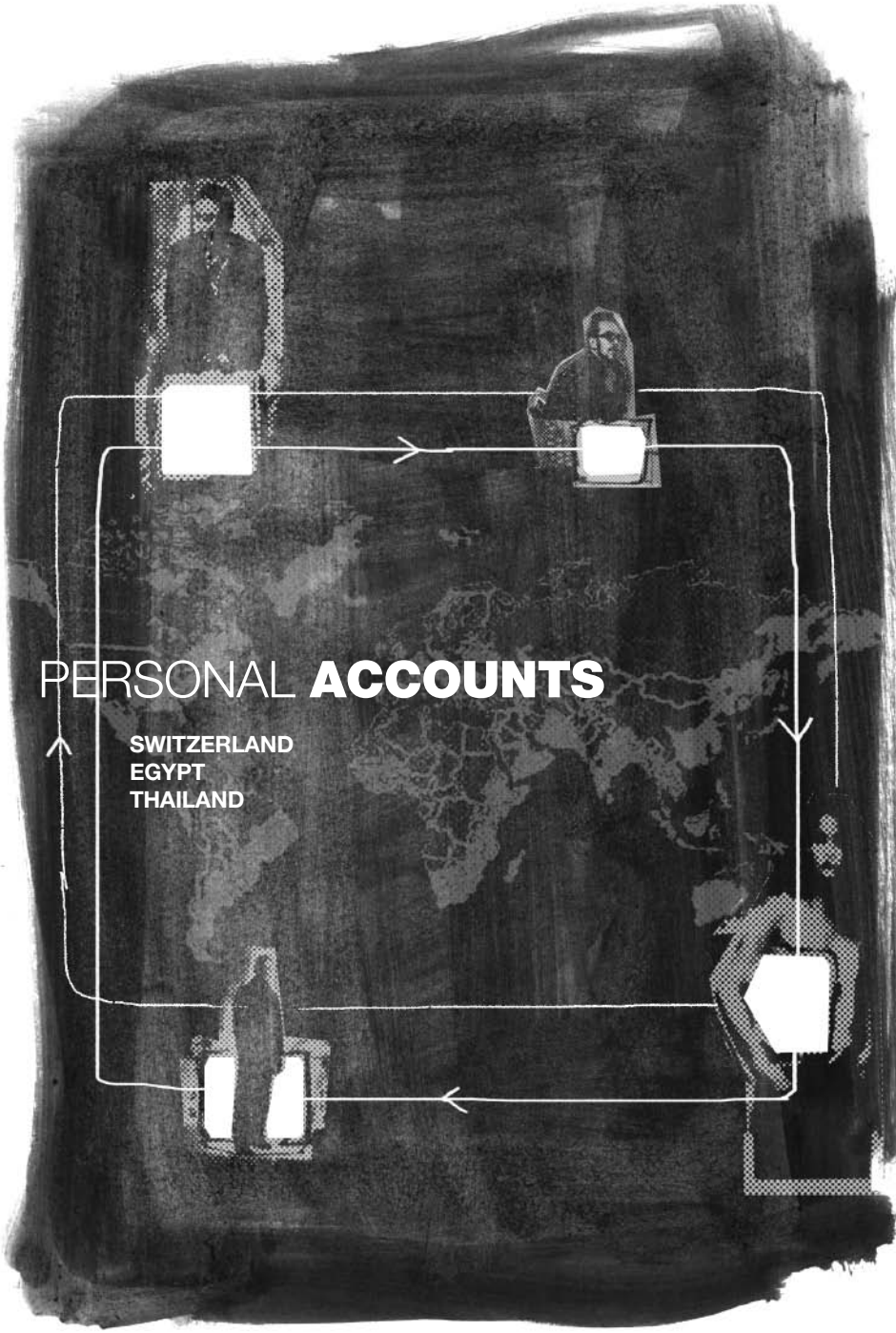




TELL TRUTH TO POWER

While many blogs include commentary, some also include original old-fashioned reporting. There's no right way to do it, but having either original reporting or an original angle on a story helps set your blog apart. Chan'ad Bahraini offered photos and audio of protests in Bahrain when an activist was jailed in November 2004. And blogger Arash Sigarchi was arrested in Iran and sentenced to 14 years in prison for criticizing the hard-line regime's arrests of other journalists. He was later freed after paying a fine, but his case is under appeal. The key is that these bloggers and so many others have spoken truth to power, and had the courage to stand up as a collective blogosphere to authorities that would rather hide the truth.

Mark Glaser is a columnist for Online Journalism Review (www.ojr.org), a publication produced by the University of Southern California's Annenberg School of Communication. He is a freelance writer based in San Francisco. You can reach him at glaze@sprintmail.com



PERSONAL **ACCOUNTS**

SWITZERLAND
EGYPT
THAILAND

SWITZERLAND

PHOTOS TO GET ROUND CENSORSHIP

By Picidae

On the Internet, we are used to dealing with text so we have chosen to take the Internet's photo.

This sign is symbol of Picidae.
Choose: it's a stylised camera or a breach in a wall.

"Picidae" comes from the Latin word meaning "peak". We wanted it to refer to the pickaxes that the East Germans used to destroy the Berlin Wall. But this sign also represents the way our project works: photographing the Internet to get round censorship.

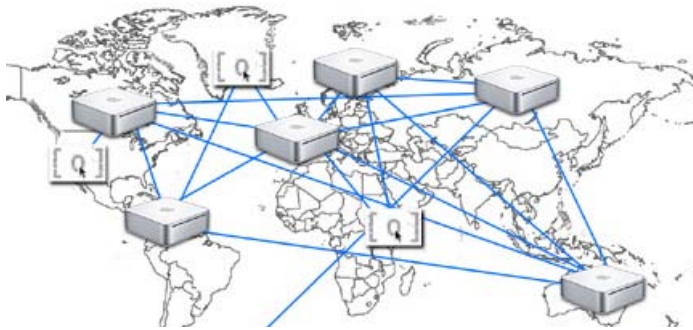
It is first and foremost an artistic project. To look at the world through this breach is to question what it is like behind the wall. It's a new way of understanding. Picidae is a new strategy: to find a way of getting round censorship which cannot be filtered or censored. This tool works for the whole network and was thought up to be based on a community of Internet-users. As the Internet is not centralised, it allows exchanges in complete freedom. That is why our project is based on an exchange of data. If certain people have their Internet access cut, Picidae will be able to use other points of access and will never be interrupted. It's also a communication platform which will allow everyone to improve technically.

We have set up "pici" servers, which allow the user to connect to the Internet via a computer which is not their own. If the user goes to a pici server, a form will come up and he can enter a web address on it. The pici server then creates a screenshot of the website

and sends it to you. To make surfing possible from this image, the server will analyse the website and integrate an exact copy with clickable areas instead of links. All the Internet links are then reproduced (menu bar, functions, search etc.) It is then possible to click on the links in the same way as on a "real" website.

In taking these images, picidae codes websites which means there is no chance of success for "key word" filtering. And to avoid the word "picidae" being filtered we have chosen a symbol which is not from any particular language. The image is universal and can thwart filtering.

To prevent censorship of requests by users on a pici server, the data entered in the forms are encrypted before being sent. Censorship systems cannot therefore know what an individual is researching, thus foiling government control.



We have tested our project in China. This journey to the ends of the Internet has shown us the extent to which censorship is hidden. Cyber-cafés are under surveillance and the

network is ultra-filtered. News about Tibet, Taiwan, political criticism and human rights are censored. One of the most important aspects of Picidae is to make censorship visible. Using pici based in Zürich, we have been able to get access to the websites we want. Picidae is currently used in China and in Europe and we plan on exporting it to Arab countries and to North Africa. The system is free and requires no installation, login or password.

Creators of the project are Christoph Wachter and Mathias Judt.

For further information http://www.picidae.net

Pici Server: http://pici.picidae.net/

Proxies are also available: contact@picidae.com: picidae is a decentralised system and does not need to be accessible through centralised data. Each point of access or server works independently from others and does not contain a name or description to avoid censorship.

EGYPT

WHEN THE LINE BETWEEN JOURNALIST AND ACTIVIST DISAPPEARS

By Wael Abbas

Blogging has allowed the limits of press freedom to be pushed back in Egypt as well as those of freedom in general. Some even consider that bloggers achieved in a few days what human rights organisations have failed to do in ten years.

By the end of 2004, movements demanding change had seen their ranks swell in the run-up to presidential elections. Demonstrations were held which were not covered by the traditional media because they were calling for the president to go. Bloggers filled the gap, by simply posting footage and photos to report on the situation. I was almost arrested as I tried to take photos of police officers who tackled them.

One day, lawyers warned me that an arrest warrant had been taken out against me because one of the shots I had posted on my blog that showed security agents destroying an Egyptian flag. But I was also accused of things I hadn't done: assaulting the security forces, attacking staff, ransacking public buildings and so on. I managed to prove that they had nothing against me but the accusations were renewed every time a demonstration was held. Ironically, I did not take part in most of the demonstrations and I was even out of the country when they took place.

Information relayed by bloggers comes from citizens. They revealed the crackdown against these peaceful demonstrations, then the rigging of elections results and brutality in police stations against people not facing any charges. That is where the line between journalist and activist disappears.

When I relayed the case of "Imad al-Kabir" (the name of the prisoner) by posting footage showing the torture of prisoners in police stations, I had the information from citizens. It is them it comes from. This case has been one of the great achievements of the blogosphere because these films, only published online, were used as evidence during the trial of police officer Islam Nabih who was sentenced to three years in prison. I am however aware that it was the work of journalists which uncovered the identity of the victims of torture. They allowed some police officers to be handed over to the courts.

The traditional media do not dare cover these subjects. Before putting out news gathered by bloggers, they make sure that they do not embarrass the government. But several newspapers have occasionally tried to appropriate recordings and photos taken by bloggers, who had them exclusively. Most of the time they do not refer to the source. Rather than submit to this situation, bloggers and journalists have started working together. A new kind of journalism has been created, which allies the two worlds.

Personally, I am satisfied if the citizen knows that a police officer has no right to assault him, if the victims of torture start talking about it, make complaints and demand their rights. All that is new in Egypt, because the security services have managed to instil fear into people and Egyptians are used to suffering in silence.

Wael Abbas is one of the leading human rights activists in Egypt. He lives in Cairo and runs a blog (http://misrdigital.blogspirit.com) on which at the start of 2007 he posted video footage exposing torture of some prisoners in Cairo police stations. This allowed the victims and the perpetrators of these crimes to be identified but also to raise awa


abcd efgh ijkl mop qrst
abcd efgh ijkl mop qrst

THAILAND

THE WEB WAS NOT DESIGNED FOR BLOGGERS

By Jotman

When I threw myself into the world of blogs in Bangkok en 2006 with my camera in my hand. I went in a taxi to the district where army tanks were guarding the main official buildings. It was just after midnight when I heard the throbbing motorbikes taking the generals to power. At dawn, the photos and video footage posted on my blog were among the first of the Thai coup to get out of the country and I continued to blog despite restrictions imposed on the Web by the military regime.

Obviously, Burma, China and other governments can always block access to my blog through the URL address, but they could also do it in other ways. The options on the platform I use, Blogger, are somewhat restrictive but that's just too bad. But if you get too involved in the design aspect you no longer always make it clear to Internet-users that you have something to say. This modest interface allows me to concentrate on what I write.

Blogging as a way of talking about the everyday can assume different forms. Often blogging is a form of "quibbling" " – going through the news with a fine-tooth comb to find the tiniest imprecision or a nugget of wisdom. Blogging is also to inform – to post news and show where it comes from. During the Burmese crisis in September 2007, I became aware of the extent of the impact my blog could have in gathering news about Burmese bloggers and their struggle. When I was trying to check out rumours about Burmese bloggers and their standard of living, I went there and interviewed a monk. After that I travelled to near the Thai border where I interviewed several other monks and pro-democracy activists. But blogging is also about publishing original and multi-media content. A blog can sometimes even be the source of a "scoop".

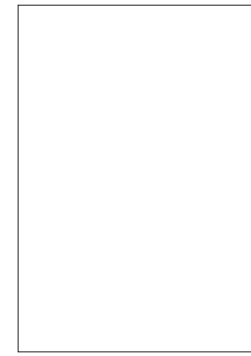
Bloggers deal with important issues, but do not have enough of an audience. The Web may very well be "as wide as the world", but it wasn't designed for bloggers. It only knows how to seek and index information. What a poor tool a search engine is for attracting new

readers! It has nothing in common with that good old newspaper which makes news available to passers-by which they would certainly not have gone to look for themselves. Everyone can read their ideal newspaper online. There is no happy chance meeting between readers and news. Paradoxically, in this era of globalisation, events are a little more linked to one another but the perspectives for readers are shrinking.

It is therefore necessary for good quality blogs to reach a wider audience. Several steps have already been taken through aggregators of blogs translated into several languages (Global Voices, Wordpress and so on). Wikipedia has also contributed to giving bloggers a certain degree of credibility. But this type of trailblazing only interests seasoned Internet-users or those specialised in a particularly part of the world. Civil society would have much to gain if it had this access.

Bloggers often find interesting information which would also have proved interesting for those who do not blog, who are neither specialists nor enthusiasts. But the network hides it away.

Jotman wants to remain anonymous. He was one of the major sources of news during the Burmese crisis and the winner of the Best of the Blogs (BOB) awards in 2007, a blog competition with which Reporters Without Borders is associated. He won his prize for his work promoting freedom of expression.



X

HOW TO BLOG **ANONYMOUSLY**

Practice with Tor and Wordpress

By Ethan Zuckerman

There are number of ways you can hide your identity when using the Internet. Any path towards anonymity needs to consider local conditions, your own technical competence and your level of paranoia. If you're worried that what you're posting could put you at risk and you're capable of installing it, posting to a blog through Tor is a very good idea. If you don't really need to be anonymous, don't be. If your name is associated with your words, people are laikely to take your words seriously. But some people are going to need ti be anonymous. Don't use these techniques unless you really need to.

And remember not to sign your blog posts with your real name !

Do you remember Sarah,who was learning the basics of anonymous blogging in 2005? Here are some reminders...

STEP ONE - PSEUDONYMS

One easy way Sarah can hide her identity is to use a free webmail account and free blog host outside her native country. (Using a paid account for either email or webhosting is a poor idea, as the payment will link the account to a credit card, a checking account or Paypal account that could be easily linked to Sarah.) She can create a new identity – a pseudonym – when she signs up for these accounts, and when the minister finds her blog, he'll discover that it belongs to "A. N. Ymous", with the email address anonymous.whistleblower@hotmail.com.

Some providers of free webmail accounts:

Hotmail
Yahoo
Hushmail - free webmail with support for strong cryptography

Some providers of free weblog hosting:

Blogsome - free WordPress blogs
Blogger
Seo Blog

Here's the problem with this strategy. When Sarah signs up for an email service or a weblog, the webserver she's accessing logs her IP address. If that IP address can be traced to her - if she's using her computer at home or her computer at work – and if the email or weblog company is forced to release that information, she could be found. It's not a simple matter to get most web service companies to reveal this information – to get Hotmail, for instance, to reveal the IP Sarah used to sign up for her account, the minister would likely need to issue a subpoena, probably in cooperation with a US law enforcement agency. But Sarah may not want to take the risk of being found if her government can persuade her email and weblog host to reveal her identity.

STEP TWO - PUBLIC COMPUTERS

One extra step Sarah could take to hide her identity is to begin using computers to make her blogposts that are used by lots of other people. Rather than setting up her webmail and weblog accounts from her home or work computer, Sarah could set them up from a computer in a cybercafé, library or university computer lab. When the minister traces the IP used to post a comment or item, he'll find the post was made from a cybercafé, where any number of people might have been using the computers.

There are flaws in this strategy as well. If the cybercafé or computer lab keeps track of who is using what computer at what time, Sarah's identity could be compromised. She shouldn't try to post in the middle of the night when she's the only person in the computer lab – the geek on duty is likely to remember who she is. And she should change cybercafés often. If the minister discovers that all the whistleblower's posts are coming from "Joe's Beer and Bits"on Main Street, he might stake someone out to watch the cybercafé and see who's posting to blogs in the hope of catching Sarah.

STEP THREE - ANONYMOUS PROXIES

Sarah's getting sick of walking to Joe's cybercafé every time she wants to post to her blog. With some help from the neighborhood geek, she sets up her computer to access the web through an anonymous proxy. Now, when she uses her webmail and weblog services, she'll leave behind the IP address of the proxy server, not the address of her home machine... which will make it very hard for the minister to find her.
First, she finds a list of proxy servers online, by searching for "proxy server" on Google. She picks a proxy server from the publicproxyservers.com list, choosing a site marked "high anonymity". She writes down the IP address of the proxy and the port listed on the proxy list.

Some reliable lists of public proxies:
• publicproxyservers.com - anonymous and non-anonymous proxies.
• Samair (http://www.samair.ru/proxy/) - only anonymous proxies, and includes information on proxies that support SSL.
• rosinstrument proxy database (http://tools.rosinstrument.com/proxy/) - searchable

database of proxy servers.

Then she opens the “preferences” section of her web browser. Under “general”, “network” or “security” (usually), she finds an option to set up a proxy to access the Internet. (On the Firefox browser, this option is found under Preferences – General – Connection Settings.)
She turns on “manual proxy configuration”, enters the IP address of the proxy server and port into the fields for HTTP proxy and SSL proxy and saves her settings. She restarts her browser and starts surfing the web.
She notices that her connection to the web seems a bit slower. That's because every page she requests from a webserver takes a detour. Instead of connecting directly to hotmail.com, she connects to the proxy, which then connects to Hotmail. When Hotmail sends a page to her, it goes to the proxy first, then to her. She also notices she has some trouble accessing websites, especially those that want her to log in. But at least her IP isn't being recorded by her weblog provider.

Sarah has another problem if she's one of very few people in the country using a proxy. If the comments on her blog can be traced to a single proxy server, and if the minister can access logs from all the ISPs within a country, he might be able to discover that Sarah's computer was one of the very few that accessed a specific proxy server. He can't demonstrate that Sarah used the proxy to post to a weblog server, but he might conclude that the fact that the proxy was used to make a weblog post and that she was one of the few people in the nation to use that proxy constituted evidence that she made the post. Sarah would do well to use proxies that are popular locally and to switch proxies often.

Here is today how Sarah’s problems can be resolved through blogging with Tor and Wordpress.

STEP ONE : DISGUISE YOU IP ADDRESS

Every computer on the internet has or shares an IP address. These addresses aren’t the same hing as physical address, but they can lead a smart system administrator to your physical address. Sarah feared that her identity would be discovered for the webserver she was accessing logs her IP address.

Thus :
1. Install Firefox
Download it at the Mozilla site (htt://www.mozilla.org) and install it on the main machine you blog from.

Why Firefox rather than Internet Explorer? Explorer has some egregious security holas that can compromise your online security (http://www.schneier.com/blog/archives/2005/12/internet_explor.html).

2. Install TOR
Download the programm from the Tor site : http://www.torproject.org/
(If access to Tor main website is blocked in your country, there are a few mirrors of it in other places where it can also be downloaded from (http://www.torproject.org/mirrors.html.en):
http://tor.cybermirror.org/
http://tor.zdg-gmbh.eu/
http://tor.anonymity.cn/

Pick the "latest stable release" for your platform and download it onto your desktop.
Follow the instructions that are linked to the right of the release you downloaded.

Tor is a very sophisticated network of proxy servers. Proxy servers request a web page on your behalf, which means that the web server doesn't see the IP address of the computer requesting the webpage. When you access Tor, you're using three different proxy servers to retrieve each webpage. The pages are encrypted in transit between servers, and even if one or two of the servers in the chain were compromised, it would be very difficult to see what webpage you were retrieving or posting to.
Tor installs another piece of software, Privoxy, which increases the security settings on your browser, blocking cookies and other pieces of tracking software. Conveniently, it also blocks many ads you encounter on webpages.

3. Install Torbutton
Turning on Tor by hand means remembering to change your browser preferences to use a proxy server. This is a multistep process, which people sometimes forget to do. Torbutton makes the process a single mouse click and reminds you whether you're using Tor or not, which can be very helpful.

if you're going to be writing primarily from shared computers (like cybercafe computers) or you're unable to install software on a computer. Download XeroBank Browser (xB Browser) or alternatively Tor on a Stick (ToaSt).

XeroBank is a highly customized version of the Firefox browser with Tor and Privoxy already installed. It's designed to be placed on a USB key so that you can access Tor from shared computers that don't permit you to install software.
Download the package from the xB Browser site onto a computer where you can save files. Insert your USB key and copy the xB-Browser.exe onto the key. Using this USB key and any Windows computer where you can insert a USB key, you can access a Tor-protected browser. On this shared computer, quit the existing web browser. Insert the key, find the key's filesystem on the Desktop, and double-click the xB-Browser_latest.exe. This will launch a new browser which accesses the web through Tor.

Test that XeroBank Browser is working by visiting the Tor test site with the Tor-enabled browser and making sure you get a "Your IP is identified to be a Tor-EXIT" message.

STEP 2 : GENERATE A NEW, HARD TO TRACE EMAIL ACCOUNT

Most web services - including blog hosting services - require an email address so that they communicate with their users. For our purposes, this email address can't connect to any personally identifiable information, including the IP address we used to sign up for the service. This means we need a new account which we sign up for using Tor, and we need to ensure that none of the data we use - name, address, etc. - can be linked to us. You should NOT use an existing email account - it's very likely that you signed up for the account from an undisguised IP, and most webmail providers store the IP address you signed up under. webmail providers store the IP address you signed up under.

1. Choose a webmail provider
Hushmail, Vaultletsoft and Gmail, but as long as you're using Tor, you could use Yahoo or Hotmail as well. Also, you can easily register a free and quick webmail account with fastmail.fm.

Hotmail and Yahoo mail both have a "security feature" that makes privacy advocates very unhappy. Both include the IP address of the computer used to send any email. This isn't relevant when you're accessing those services through Tor, since the IP address will be a Tor IP address, rather than your IP address. Also, Hotmail and Yahoo don't offer secure HTTP (https) interfaces to webmail - again, this doesn't matter so long as you use Tor every time you use these mail services. But many users will want to check their mail in circumstances where they don't have Tor installed - for your main webmail account, it's worth choosing a provider that has an https interface to mail.

Hushmail provides webmail with a very high degree of security. Their interface to webmail uses https and they don't include the sending IP in outgoing emails. But they're a for-profit service and they offer only limited services to non-paying users. If you sign up for a free account, you have to log into it every couple of weeks to make sure the system doesn't delete it. Because they're aggressive about trying to convert free users to paid users, and because their system uses a lot of Java applets, some find that Hushmail isn't the right choice for them.

Gmail, while it doesn't advertise itself as a secure mail service, has some nice security featuresbuilt in. If you visit this special URL, your entire session with Gmail will be encrypted via https.

2. Register your new account
Don't use any personally identifiable information - consider becoming a boringly named individual in a country with a lot of web users, like the US or the UK. Set a good, strong password (at least eight characters, include at least one number or special character) for the account and set a good, strong password, at least eight characters, include at least one number or special character.
Choose a username similar to what you're going to name your blog.

3. Test if it works!
Make sure you're able to log onto the mail service and send mail while Tor is enabled. It is most likely that Tor changes its circuit every 10 minutes and this could disrupt your web-mail operations, so you should consider limiting the process of writing a new email to 10 minutes.

STEP 3 : REGISTER YOUR NEW ANONYMOUS BLOG

You'll have to be very careful by creating that blog. It requires more attention and caution than creating a non anonymous blog.

TURN TOR ON IN YOUR BROWSER, OR START XEROBANK

Visit Wordpress.com and sign up for a new account by clicking the "Get a New WordPress Blog" link. Use the email address you just c r e a t ed and c r e a t e a us e rname tha t wi l l be pa r t of your blog addr e s s : thenameyouchoose.wordpress.com
Wordpress will send an activation link to your webmail account. Use your Tor-enabled browser to retrieve the mail and follow that activation link. This lets Wordpress know you've used a live email account and that they can reach you with updates to their service - as a result, they'll make your blog publicly viewable and send you your password. You'll need to check your webmail again to retrieve this password.
Still using Tor, log into your new blog using your username and password. Click on "My Dashboard", then on "Update your profile or change your password." Change your pass-word to a strong password that you can remember. Feel free to add information to your profile as well… just make sure none of that information is linked to you!

STEP 4 : POST TO YOU BLOG

Write your blog post offline. Not only is this a good way to keep from losing a post if your browser crashes or your net connection goes down, it means you can compose your posts somewhere more private than a cybercafe. A simple editor, like Wordpad for Windows, is usually the best to use. Save your posts as text files (After blogging, always remember to remove these files from your machine completely, using a tool like Eraser or

Ccleaner which is is available in many languages and wipes te porary files automatically from all installed browsers and other applications).

Turn on Tor, or use XeroBank, and log onto Wordpress.com. Click the “write” button to write a new post. Cut and paste the post from your text file to the post window. Give the post a title and put it into whatever categories you want to use.
Before you hit “Publish”, there’s one key step. Click on the blue bar on the right of the screen that says “Post Timestamp.” Click the checkbox that says “Edit Timestamp”. Choose a time a few minutes in the future - ideally, pick a random interval and use a different number each time. This will put a variable delay on the time your post will actually appear on the site Wordpress won’t put the post up until it reaches the time you’ve specified.

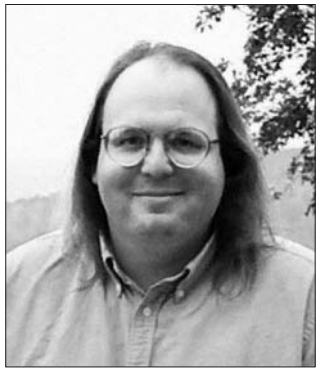
By changing the timestamp of the posts, we make an attack more difficult for the internet service provider. Now they’d need access to the logs of the Wordpress server as well, which are
much harder to get than their own logs. It’s a very easy step to take that increases your security.

STEP 5 : COVER YOUR TRACKS

Securely erase the rough drafts of the post you made from your laptop or home machine. If you used a USB key to bring the post to the cybercafe, you’ll need to erase that, too. It’s not sufficient to move the file to the trash and empty the trash - you need to use a secure erasing tool like Eraser or Ccleaner which overwrites the old file with data that makes it impossible to retrieve. On a Macintosh, this functionality is built it - bring a file to the trash and choose “Secure Empty Trash” from the Finder Menu.

Clear your browser history, cookies and passwords from Firefox. Under the Tools menu, select “Clear Private Data”. Check all the checkboxes and hit “okay”. You might want to set up Firefox so that it automatically clears your data when you quit - you can do this under “Firefox -> Preferences -> Privacy -> Settings”. Choose the checkbox that says “Clear private data when closing Firefox”. In case you cannot install programs on the computer, use the IE Privacy Cleaner tool from the USB stick to wipe temp browser data.

ETHAN ZUCKERMAN



Ethan Zuckerman is a fellow at the Berkman Center for Internet and Society at Harvard Law School where his research focuses on the relationship between citizen journalism and conventional media, especially in the developing world. He's a founder and former director of Geekcorps, a non-profit organization that focuses on technology training in the developing world, and was one of the founders of webhosting company Tripod.

TECHNICAL WAYS TO GET ROUND CENSORSHIP

By Nart Villeneuve

CONTENTS

INTERNET CONTENT FILTERING

Filtering technology allows controls to be placed on access to Internet content. Although the initial focus of such technology was on the individual level – allowing parents to restrict children's access to inappropriate content – filtering technology is now being widely deployed at institutional and national level. Control over access to Internet content is becoming a priority for a number of institutional actors including schools, libraries and corporations. Increasingly, filtering technology is being deployed at national level. Access to specific Internet content is being blocked for entire populations, often with little accountability.

Content filtering technologies rely on list-based blocking, often in conjunction with blocking techniques that use keyword matching, to dynamically block Internet content. Lists of domain names and URLs are compiled and categorized then loaded into filtering

software which can be configured to block only certain categories. When users try to access a web page, the filtering software checks its list database and blocks access to any web page on that list. If keyword blocking is enabled, the software will check each web page (the domain, URL path and/or body content of the requested page) and dynamically block access to the web page if any of the banned keywords are present.

Filtering systems are prone to two inherent flaws: over-blocking and under-blocking. They often block access to wrongly classified content and often do not block all access to the content they intend to block. But the key issue is the secrecy surrounding the creation of lists of websites that are blocked by filtering technologies. Although there are some open source lists (focusing mostly on pornography), commercial filtering lists and lists deployed at national level are secret. Commercial lists of categorized domains and URLs are the intellectual property of their manufacturers and not made public. Despite the fact that some filtering software manufacturers make online URL checkers available, the block lists as a whole are secret and unavailable for independent scrutiny and analysis.

Often countries will build on commercial filtering technology lists adding specific websites pertinent to their respective countries. Blocked sites most often include opposition political parties or newspapers, human rights organizations, international news organizations and content critical of the government. Most countries focus on local language content, as opposed to English sites, and increasingly target interactive discussion sites such as web blogs and web forums.

CIRCUMVENTION TECHNOLOGIES

In response to state-directed Internet filtering and monitoring regimes, many forms of circumvention technologies have emerged to allow users to bypass filtering restrictions. There are numerous projects to develop technologies that would enable citizens and civil society networks to secure themselves against, or work around, Internet censorship and surveillance. These tools as are referred to as "circumvention technologies." In general, circumvention technologies work by routing a user's request from a country that implemented filtering through an intermediary machine that is not blocked by the filtering regime. This computer then retrieves the requested content for the censored user and transmits the content back to the user. Sometimes, these technologies may be specifically designed for a particular filtering situation or customized for a specific country. Other times, users may simply adapt existing technologies for circumvention purposes even though that may not be the original purpose of the technology.

Some of these technologies are developed by private companies, others by ad-hoc groups of hackers and activists. They range from small, simple scripts and programs to highly-developed peer-to-peer network protocols. Given the range of the technologies involved it is necessary for potential users to be able to weigh the strengths and weaknesses of specific techniques and technologies so as to choose the appropriate circumvention technologies that suit their needs.

There are two users of circumvention technologies: the circumvention provider and the circumvention user. The circumvention provider installs software on a computer in a non-filtered location and makes this service available to those who access the Internet from a censored location. Thus successful circumvention relies on meeting the specific needs of both users.

This paper aims to inform users who have made the decision to use circumvention technologies of the available options and how to assess which is best suited to the specific needs of the user. This is done by determining the needs and capacity of the users involved – those using as well as those running the circumvention technology – while balancing the appropriate level of security with the technologies' usability by the end-user. Effective, secure, and stable circumvention is achieved by matching the right technology with the right user.

DETERMINING NEEDS AND CAPACITY

Circumvention technologies often target different types of users with varying resources and levels of expertise. What may work well in one scenario may not be the best option in another. When choosing a circumvention technology it is important for the potential circumvention provider and user to ask these questions :

What is the number of expected users and the available bandwidth? (for the circumvention provider and the user).
Where is the primary point of Internet access for the expected user(s) and what will they be using it for?
What is the level of technical expertise? (for the circumvention provider and the user).
What is the availability of trusted out-of-country contacts for the end-user?
What is the level of expected penalty if the user is caught using circumvention technology ?
• Does the end-user properly understand the potential security risks of using the specific circumvention technology?

NUMBER OF USERS AND AVAILABLE BANDWIDTH

The circumvention provider needs to estimate the number of users the circumvention technology is intended for and balance that with the available bandwidth. The end-user must also take into account their bandwidth as circumvention technology will slow their Internet use.

People interested in running public proxies need to consider that their circumventor may be used by persons who are not in censored locations. For example, circumventors may be used to download entire movies which will use a lot of bandwidth. Therefore you may wish to restrict access to your circumventor or how much total bandwidth you'd like to circumventor to be restricted to. Different available technologies provide some or all of these options.

PRIMARY POINT OF ACCESS AND USE

There will be varying options of applicable circumvention technologies depending on where the end-users access the Internet and what services they need to run through the circumvention system. For example, users who access the Internet from public computers or Internet cafés may not be able to install any software and will be restricted to web-based solutions. Others may want to use applications besides Web browsing (HTTP), such as e-mail (SMTP) and file transfers (FTP), and thus may want to install software on their computer workstation and to tweak their computer's settings. Of course, this requires a certain level of technical skill on the part of that user.

LEVEL OF TECHNICAL EXPERTISE

The greater the level of technical expertise (and limited number of users) the more circumvention options increase. The barriers to non-technical users include the installation and set-up process as well as any configuration changes or extra steps that must be taken when actually using the circumvention technology. This applies to both the circumvention provider and the end-user. The incorrect use of circumvention technology may put users at avoidable risk.

AVAILABILITY OF TRUSTED CONTACTS

End-users can greatly enhance their circumvention options if they know and trust persons outside their country. If a user does not have a trusted contact then their options are limited to publicly available systems and if the user can locate these systems so can those implementing the filtering and blocking. With a trusted contact the end-user can consult with the circumvention provider to find a solution that meets their specific needs and can be kept private to avoid detection. Successful, long-term and stable circumvention is greatly enhanced by having a trusted contact in a non-filtered location.

THE EXPECTED PENALTY

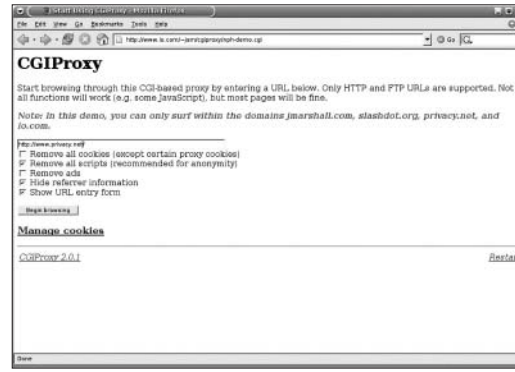
It is extremely important to know the penalty users face if they are caught using circumvention technology. Depending on the severity, options will vary. If the legal environment is lax and the expected penalty low, users can choose from a variety of options which, while effective at circumvention, are not very secure. If the environment is extremely dangerous, care must be taken to implement technologies that are both discreet and secure. Some may even be used with a legitimate cover story or other forms of obfuscation.

SECURITY RISKS

Too often users are encouraged to use circumvention technology without being properly informed of the potential security risks, which can be minimized by deploying the right technology in the right place and used correctly by the end-user.

WEB-BASED CIRCUMVENTORS

Web-based circumventors are special web pages that contain a web form that allows users to simply submit a URL and have the web-based circumventor retrieve the content of the requested web page and display it to the user. There is no connection between the user and the requested website, and the circumventor transparently proxies the request allowing to user to browse blocked websites seamlessly. Web-based circumventors also re-write the links in the requested web page to point back through the circumventor itself so that the user can continue web surfing normally. When using a web-based circumventor, the end-user does not have to install any software or change any of their browser settings. All the end-user has to do is visit the URL of the circumventor, enter the URL they wish to visit in the form located on the circumventor page and press the submit button. (Web-based circumventors may look different from one another but the basic functionality is the same). Thus no level of expertise is required and it can be used from any point of access.



Proxy servers / change the navigator settings

Advantages :
Web-based circumvention systems are easy to use and no software needs to be installed at the end-user level.
Public web-based circumvention services are available to users who do not have a trusted contact in an unfiltered location.
Private web-based circumvention systems can be customized to meet the specific circumvention needs to users and are less likely to be found by the filtering authorities.

Disadvantages :
Web-based circumvention systems are often restricted to web traffic (HTTP) and may not be accessible by encrypted access (SSL). Web services (such as web-based email) that require authentication may not be fully functional.
Public web-based circumvention services are generally well known and may already be blocked. Most of these services are already blocked by commercial filtering software.
Private web-based circumvention systems require that a user have a contact in an unfiltered location. Ideally, the two parties must be able to communicate in some way that isn't easily monitored.

PUBLIC WEB-BASED CIRCUMVENTION SERVICES

There is publicly available web-based circumvention software as well as services. Most provide free service while some have more options, such as encrypted access, available with a paid subscription. Some are operated by companies, others by volunteers as a public service. A few examplzs:

http://www.anonymizer.com/	http://www.guardster.com/
http://www.unipeak.com/	http://www.webwarper.net/
http://www.anonymouse.ws/	http://www.proximal.com/
http://www.proxyweb.net/	http://www.the-cloak.com/

Since the web addresses of these services are widely known, most Internet filtering applications already have these services on their block lists as do many countries that filter at national level. If the web addresses of these services are blocked they cannot be used. Also, many public web-based circumventors do not encrypt the traffic between the circumventor and the end-user. Any information transmitted by the user can be intercepted by the operator of the circumvention service.

Public Web-based circumvention services are best suited for users in low security risk environments who are without trusted contacts in non-filtered locations and have temporary or ad-hoc circumvention needs and who do not need to transmit sensitive information.

WEB-BASED CIRCUMVENTION SOFTWARE

Installation of web-based circumvention software can require some level of technical expertise and appropriate resources (a web server and bandwidth). With a private circumventor, the location is only made known to the intended users whereas public circumventors and anonymity services are known to both users and those implementing filtering (and are on most commercial filtering software's blocklists). The chances of private circumventors being detected are blocked and lower than that of public circumvention services.

Private circumventors can be set up with some level of customization tailored to the specific needs of the end-user. Some common customizations are changing the port number that the web server runs on and implementing encryption. Secure Sockets Layer (SSL) is a protocol for transmitting content securely over the Internet. It is often used by websites to securely transmit information, such as credit card numbers. SSL-enabled websites are accessed with "HTTPS" instead of the normal "HTTP".

Another option when using SSL is creating an innocuous web page at the root of the web server and concealing the circumventor with a random path and file name. Although an intermediary may be able to determine the server the user is connecting to, they will not be able to determine the requested path because that part of the request is encrypted. For example, if a user connects to "https://example.com/secretcircumventor/" an intermediary will be able to determine that the user connected to example.com but they will not know that the user requested the circumventor. If the circumventor operator places an innocuous page at example.com, then even if any monitoring is occurring the circumventor will not be discovered.

- CGIProxy: A CGI script acts as an HTTP or FTP proxy.
  http://www.jmarshall.com/tools/cgiproxy
- Peacefire's Circumventor: An automated installer program that makes it much easier for non-technical users to install and configure CGIProxy.
  http://www.peacefire.org/circumventor/simple-circumventor-instructions.html
- pHproxy: An experimental, highly configurable web-based circumventor.
  http://ice.citizenlab.org/projects/phproxy
- Psiphon: An SSL-enabled webserver with built-in web-based circumventor.
  http://psiphon.civisec.org

Private web-based circumventors, with encryption enabled, are best suited for users that require stable circumvention services for web traffic and have trusted contacts in non-filtered locations that have sufficient technical skills and available bandwidth to set up and maintain the web-based circumventor. This is the most flexible circumvention option available for simple web traffic and is least likely to be discovered and blocked.

WEB-BASED CIRCUMVENTION: SECURITY CONCERNS

Circumvention systems do not necessarily provide anonymity. Although the end-users identity is shielded from the operators of the websites visited. If the session between the user and the web-based circumventor is in plain text (HTTP), as with most free services, the content can be easily intercepted and analyzed by an intermediary such as an Internet service provider (ISP). So although circumvention may be successful, the authorities can still track the fact that the user has visited and used a web-based circumventor. Moreover they can determine what content, including what websites the user visited, was exchanged between the web-based circumventor and the end-user.

Web-based circumventors that operate in plain text mode (non-encrypted) sometimes use URL obfuscation to counter filtering conducted by looking for key words in Uniform Resource Locators (URL). For example, using a simple technique such as ROT-13, where the current letter is replaced by the one 13 characters ahead of it in the alphabet, the URL http://ice.citizenlab.org becomes uggc://vpr.pvgvmrayno.bet. In effect, the text of the URL is encoded so that the key words the filtering technology is scanning for will not be present in the requested URL. However, the content of the session can still be sniffed even if the circumvention was successful.

There are also risks concerning the use of cookies and scripts. Many web-based circumventors can be configured to remove cookies and scripts, but many sites (e.g. webmail sites) require the use of cookies and scripts. Care should be taken when enabling these options. Another related risk, especially when using services that require logins/passwords, is accessing the circumventor through a plaintext connection and then using it to request information from an encrypted server. In this scenario, the circumventor retrieves the request information from the SSL-enabled server through an encrypted transmission, but then sends the contents in plain text back to the user, thus exposing the sensitive information to possible interception.

Some of these security issues can be solved by using web-based proxies through an encrypted connection. Some web-based proxies are configured to be access using SSL (HTTPS), which encrypts the connection between the end-user and the web-based circumventor. In this scenario, intermediaries can only observe the fact that the user has connected to the web-based circumventor and cannot determine the content of the session. It is highly recommended that users ensure they use SSL-enabled web-based circumventors if the security risks are high.

However, although the end-user's connection to the web-based circumventor may be secure, any information passing through a web-based circumventor can be intercepted by the owner of the web-based circumventor. An additional security concern is the records that the circumvention provider keeps. Depending on the circumventor's location, or the location of their server, authorities may have access to their log files.

There are still some concerns that users should be aware of, even when using SSL-enabled web-based circumventors. One is that using encryption may draw extra attention to the users' circumvention activities, and the use of encryption may not be legal in all locations. Also, it may be possible for the filtering authorities to determine what websites a user visits through a web-based circumventor, even when using SSL encryption using techniques known as HTTPS fingerprinting and Man-In-The-Middle (MITM) attacks. However, pages with dynamic content or circumventors that add random amounts of decoy text or images to requested content can reduce this technique to a level of insignificant risk. If users are provided with the "fingerprint", or security signature, of the SSL certificate they can manually verify that the certificate is in fact authentic, thus avoiding the MITM attack (1).

PROXY SERVERS

A "proxy server" is a server that is situated between a client, such as a web browser, and a server, such as a web server. The proxy server acts a buffer between the client and the server and can support a variety of data requests including web traffic (HTTP), file transfers (FTP) and encrypted traffic (SSL). Proxy servers are used by individuals, institutions, and states for a variety of purposes including security, anonymity, caching and filtering. To use a proxy server, the end-user must configure the settings of their web browser with the IP address or hostname of the proxy server as well as the port number that the proxy server is running on. While this is fairly simple, it may not be possible to modify browser settings in public Internet access locations such as libraries, Internet cafés and workplaces.

1 For more on potential attacks on circumvention systems, see Bennett Haselton's article ("List of possible weaknesses in systems to circumvent Internet censorship") at http://peacefire.org/circumventor/list-of-possible-weaknesses.html and a reply by Paul Baranowski at: www.peek-a-booty.org/pbhtml/downloads/ResponseToLopwistcic.pdf

Advantages:
There are many software packages to choose from that can transparently proxy traffic in addition to web traffic (HTTP) and can be configured to operate on non-standard ports.
There are many publicly accessible proxy servers.

Disadvantages:
Most proxy servers are not enabled with encryption by default, therefore the traffic between the user and the proxy is not secure.
The user must have the necessary permissions to change the browser settings, and if ISP's require that all traffic go through the ISP's proxy server it may not be possible to use an open proxy server.
The scanning for and use of publicly accessible proxy servers may be illegal and these proxies may become unavailable to the user at any time.

PROXY SERVER SOFTWARE

Proxy server software can be installed by trusted contacts with some degree of technical expertise located outside of the country that filters. Proxy server software should be installed in locations where there is plenty of available bandwidth and should be configured to use encryption technology. It is especially useful for situations in which an office or small organization is in need of a stable circumvention solution. After users in the filtered locations configure their browsers to point through the proxy server they can transparently surf the Internet. While not the most stealthy circumvention solution, private proxy servers are a more robust solution than web-based proxy systems. Proxy servers are better than web-based proxies at seamlessly proxying sites that require authentication and cookies, such as web mail sites. The proxy servers can also be customized to meet the specific needs of the end-user and adapt to the local filtering environment.

- Squid is free proxy server software and can be secured with Stunnel server.
  http://www.squid-cache.org
  http://www.stunnel.org
  http://ice.citizenlab.org/projects/aardvark
- Privoxy is a proxy with advanced filtering capabilities for protecting privacy.
  http://www.privoxy.org
- Secure Shell (SSH) has a built-in socks proxy ($ ssh -D port secure.host.com)
  http://www.openssh.com
- HTTPport/HTTPhost allows you to bypass your HTTP proxy, which is blocking you from the Internet.

Private proxy servers with encryption enabled are best suited for groups or users in an office environment that require a permanent, stable circumvention solution and have trusted contacts with sufficient technical skills and available bandwidth outside the country to install and maintain the proxy server.

PUBLICLY ACCESSIBLE PROXY SERVERS

Open proxies are servers that are intentionally or otherwise left open for connections from remote computers. It is not explicitly known if open proxy servers have been set up as a public service or if they have been just badly configured to inadvertently allow public access.

WARNING: Depending on the interpretation of local law, the use of open proxy servers may be viewed as 'unauthorized access' and open proxy users may subject to legal penalties. The use of open proxy servers is not recommended.

Locating open proxies

Many websites maintain lists of open proxy servers, but this not a guarantee that the proxy service is still available. Nothing guarantees that the information on these lists, especially information concerning anonymity level and geographical location of the proxy, is accurate. Be aware that you are using these services at your own risk.

Open proxy list websites:

http://www.samair.ru/proxy/
http://www.antiproxy.com/
http://tools.rosinstrument.com/proxy/
http://www.multiproxy.org/
http://www.publicproxyservers.com/

Software: ProxyTools/LocalProxy

http://proxytools.sourceforge.net

Open proxies: uncommon ports

Some countries that filter at national level block access to standard proxy ports. A "port" is a logical connection location used by specific protocols. Different Internet services pass data through on particular port numbers. Certain port numbers are assigned, by the Internet Assigned Numbers Authority (IANA), to specific protocols or services. For example, port 80 is reserved for HTTP traffic. When you access a website in your browser you are actually connecting to a web server running on port 80. Proxy servers also have ports that are assigned to them by default. Therefore many filtering technologies will not allow access to these ports. Therefore successful circumvention may require use of a proxy that has been configured to operate on a non-standard port.

http://www.web.freerk.com/proxylist.htm

PROXY SERVERS: SECURITY CONCERNS

The configuration of proxy servers is extremely important because it controls the security or anonymity of a connection. In addition to the lack of use of encryption, proxy servers may pass information about the end-user to the server the content has been requested from that can be used to identify the IP address of the computer initiating the request for content. Moreover, all the communication between you and the proxy server may be in plain text, thus easily intercepted by upstream filtering authorities. And any information passing through the proxy server can be intercepted by the owner of the proxy server.

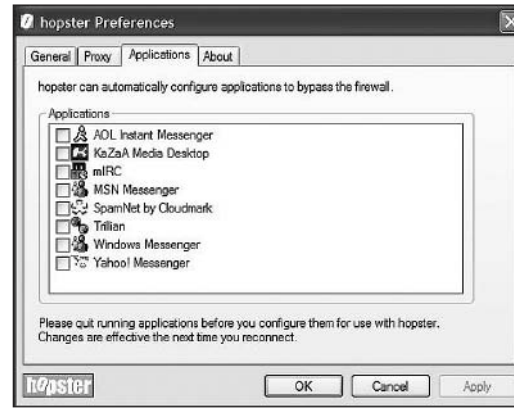
The scanning for and use of publicly accessible proxy servers is not recommended. Open proxy servers are often used due to their availability but they do not provide any security despite the fact that they may be able to successfully circumvent Internet filtering.

As with web-based proxies, proxy servers are subject to the same security concern. Harmful scripts and cookies will still be transmitted to the end-user and even if used in conjunction with encryption technology, proxy servers can also be subject to MITM and HTTPS fingerprinting attacks. It should also be noted that some browsers will leak sensitive information when using a socks proxy, a particular type of proxy server capable of handling other types of traffic in addition to web traffic. When making a request for a website the domain name is translated into an IP address. Some browsers do this locally so the process is not directed through the proxy. In these cases, the request for the blocked website's IP address will be handled by Domain Name System (DNS) servers in the country that implements filtering (2).

2 For more, see the Tor site: http://tor.eff.org/cvs/tor/doc/CLIENTS

The use of open, publicly accessible proxy servers is not usually advisable and should only be used by people in low security risk environments with temporary or ad-hoc anonymity needs and who do not need to transmit sensitive information.

TUNNELING



Tunneling software

Tunneling, also known as port forwarding, allows one to encapsulate insecure, unencrypted traffic within an encrypted protocol. The user in a censored location must download client software that creates a tunnel to a computer in a non-filtered location. The normal services on the user's computer are available, but run through the encrypted tunnel to the non-filtered computer which forward the user's requests and their responses transparently. Various tunneling products are available. Users with contacts in a non-filtered country can set up private tunneling services while those without contacts can purchase commercial tunneling services, usually by monthly subscription.

When using free tunneling services users should note that they often include advertisements. Requests for the advertisements are conducted through plain text HTTP requests which can be intercepted by any intermediary who can then determine that the user is using a tunneling service. Moreover, many tunneling services rely on the use of socks proxies which may leak domain name requests.

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

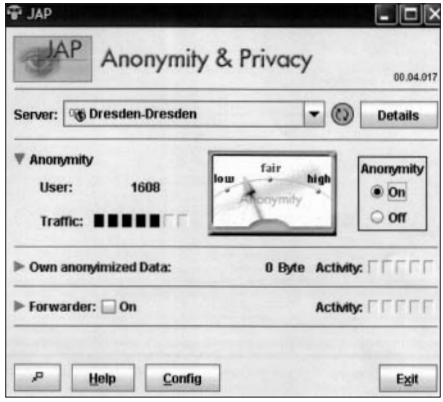
Advantages:
Tunneling applications provide encrypted network transfer.
Tunneling applications generally have the ability to securely proxy many protocols, not just web traffic.
There are existing commercial services that users who do not have contacts in non-filtered countries can purchase.

Disadvantages:
Commercial tunneling services are publicly known and may already be filtered.
Tunneling applications cannot be used by users in public access locations where users cannot install software, such as Internet cafés or libraries.
Use of tunneling applications may require a higher level of technical expertise than other circumvention methods.

Tunneling applications are best suited for technically capable users that require secure (but not anonymous) circumvention services for more than just web traffic and do not access the Internet from public locations. Commercial tunneling services are an excellent resource for users in censored countries that do not have trusted contacts in non-filtered locations.

ANONYMOUS COMMUNICATIONS SYSTEMS

Circumvention technologies and anonymous communications systems are similar and often inter-related but operate under distinctly different criteria. Anonymous communications systems focus on ensuring the privacy of the user by shielding the identity of the requesting user from the content provider. In addition, advanced systems employ a variety of routing techniques to ensure that the user's identity is shielded from the anonymous communications system itself. Circumvention systems do not necessarily focus on anonymity. Instead, the focus is on secure communications to bypass specific restrictions imposed on the users' ability to send and receive Internet communications. Bypassing content restrictions requires secure communications technology and often a degree of stealth but not necessarily anonymity.
Anonymous communications systems are often used for circumvention. One advantage of them is that there are several existing networks that can be immediately tapped into and used to bypass content restrictions with the added benefit of being able to do so anonymously.



The use of anonymous communications systems for circumvention is restricted to computers on which the user has the appropriate permissions to install software. Persons who access the Internet through public terminals, libraries or Internet cafés will most likely be unable to use such systems for circumvention. They may also slow down connection speeds.

Users seeking to bypass Internet filtering at national or ISP level may find the filtering authorities take steps to block the use of anonymous communications systems. If the system being used operates on a static port, filtering software can easily be configured to deny access. The more well-known the anonymous communications system, the greater the risk that it will be blocked. In addition, to combat systems that rely on the use of peers or publicly known nodes the filtering authorities can simply deny access to these hosts. The filtering authorities may operate a node of their own and attempt to monitor users who try to connect to it. In some restrictive environments where traffic to these well-known systems is monitored, the use of such systems may draw attention to users (3).

Advantages:
They provide both security and anonymity.
They generally have the ability to securely proxy many protocols, not just web traffic.
They often have a community of users and developers who can provide technical assistance.

Disadvantages:
They are not specifically designed for circumvention. They are publicly known and may be filtered easily.
They cannot be used by users in public access locations where users cannot install software, such as Internet cafés or libraries.

• Tor is a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet. It also enables software developers to create new communication tools with built-in privacy features. Tor provides the foundation for a range of applications that allow organizations and individuals to share information over public networks without compromising their privacy.
http://tor.eff.org
• JAP makes it possible to surf the Internet anonymously. Instead of connecting directly to a web server, users take a detour, connecting with encryption through several intermediaries, so-called mixes.
o http://anon.inf.tu-dresden.de/index_en.html
• Freenet is free software which lets you publish and obtain information on the Internet without fear of censorship. It is entirely decentralized and publishers and consumers of information are anonymous.
http://freenet.sourceforge.net

3 For more on potential attacks on circumvention systems, see Bennett Haselton's article ("List of possible weaknesses in systems to circumvent Internet censorship") at http://peacefire.org/circumventor/list-of-possible-weaknesses.html and a reply by Paul Baranowski at: www.peek booty.org/pbhtml/downloads/ResponseToLopwistcic.pdf

Use of such systems may require quite a high level of technical expertise. Anonymous communications systems are best suited for technically capable users who require both circumvention and anonymity services for more than just web traffic and do not access the Internet from public locations.

CONCLUSION

The decision to use circumvention technology should be taken seriously, carefully analyzing the specific needs, available resources and security concerns of the end-user. There is a wide variety of technologies available for users who want to circumvent Internet filtering. However, using them for successful and stable circumvention service depends on a variety of factors, including the user's level of technical skill, potential security risk, and contacts available outside the censored country. Governments may also take counter-measures to effectively block specific circumvention technologies.

The keys to successful and stable circumvention capability are trust and performance. Circumvention systems need to be targeted to users in specific circumstances or be readily adaptable to the needs of the end-user. They need to be secure, configurable and often stealthy. Trust should be established between circumvention provider and the end-user by understanding the specific legal and political environment in which the end-user operates and being up-front about the limitations of circumvention technologies.

Nart Villeneuve is the director of technical research at the Citizen Lab, an interdisciplinary laboratory based at the Munk Centre for International Studies at the University of Toronto. As both a software developer and academic, he is currently working with the OpenNet Initiative (ONI), documenting Internet content filtering and surveillance practices worldwide. He has also been working on documenting and evaluating existing circumvention technology as well as developing circumvention technology. In addition to Internet censorship, his research interests include hacktivism, cyberterrorism and Internet security. Nart Villeneuve is a recent graduate of the University of Toronto's Peace and Conflict Studies program.

Acknowledgements
Michelle Levesque, Derek Bambauer and Bennett Haselton.

ENSURING YOUR **E-MAIL IS TRULY PRIVATE**

By Ludovic Pierrat

Most governments now have the means to spy on electronic messages. The "cyberpolice" in repressive countries use it to spot and arrest political opponents and many Internet users have been thrown in prison for sending or even just forwarding an e-mail. A political dissident in the Maldives was given a 15-year jail sentence in 2002 for corresponding by e-mail with Amnesty International. An Internet user in Syria has been in prison since February 2003 for forwarding an e-mail newsletter.

So here are some tips on how to ensure your e-mails remain private.

Using the e-mail account supplied by your Internet service provider (ISP), such as AOL, Wanadoo or Free, or by a firm doesn't guarantee any e-mail confidentiality. The owners of the networks your messages pass through can very easily intercept them. When the authorities in any country want to investigate Internet users, they usually go through their ISP to read their e-mail.

A "webmail" account (such as Yahoo! or Hotmail) is more secure because it doesn't use the servers of a local ISP. To read webmail messages, you have to force your way in or intercept messages as they're being transmitted, which is technically more difficult. Unfortunately this protection is only relative, since police experts or hackers can easily look at your webmail.

Encryption (writing protected by a code) is the main way to really ensure the privacy of your messages. There are two kinds.

CLASSIC ENCRYPTION

Ann and Michael want to exchange secret messages, so they agree on an encryption and decryption code and a key. Then they exchange messages using them.

The snag with this method is that if a third person intercepts the messages in which Ann and Michael exchange their key, that person can see it and use it, perhaps to send bogus e-mails to Ann and Michael. So Ann and Michael have to exchange their key when nobody else can see it, by meeting in person, for example.

ASSYMETRIC ENCRYPTION

The best way to fix the problem is to use "asymmetric" encryption. Two keys are needed for this, one to encrypt, the other to decrypt. Details of the encrypting key (the "public key") can be exchanged without risk over the Internet because it can't be used to decrypt messages. The decrypting key (the "secret key") must never be communicated.

With asymmetric encryption, Ann has her own pair of keys (a public key that she gives out and a secret one that she keeps). Ann sends her key to Michael, who uses it to encrypt his messages to her. Only Ann, with her secret key, can then decrypt Michael's messages. Michael, with his own pair of keys, in turn sends his public key to Ann, who can then reply to his messages in complete privacy.

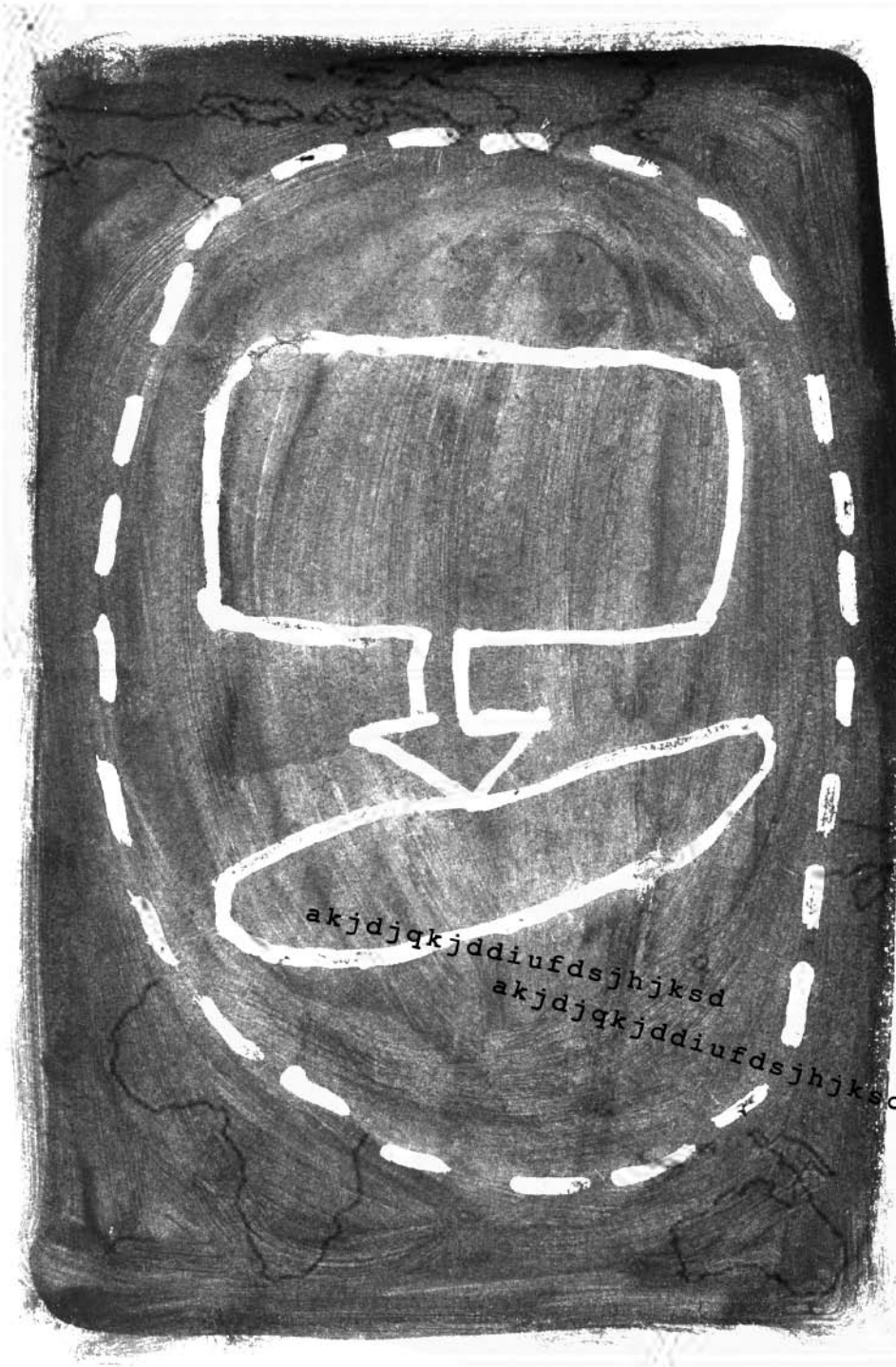
But since the public key is exchanged over the Internet without special protection, it's best to check its validity with its owner. Each key has a "fingerprint" (a short string of characters), which it's easy to communicate in person or over the phone.

An unverified key may be a false one issued by a third person with evil intent, making the encryption totally useless. The reliability of assymetric encryption depends entirely on protecting the secret key and checking the public key of the other person.

OpenPGP (Open Pretty Good Privacy) is the standard asymmetric encryption. The most popular software to create and use a pair of keys and manage the public keys of its correspondents is GnuPG (GNU Privacy Guard), which can be used both with mail programmes such as Thunderbird or Outlook, with webmail or with instant messaging.

Download GnuPG at : www.gnupg.org
Download special version for Windows at : www.winpt.org

Ludovic Pierrat is a computer engineer who runs Wa Company, an information technology consultancy and production firm.


akjdjqkjddiufdsjhjksd
akjdjqkjddiufdsjhjksd

THE 2008 GOLDEN SCISSORS OF CYBER-CHAMPIONSHIP

By Clothilde Le Coz

Most of the world's authoritarian regimes are trying to control what their citizens read and do online. They're getter better and better at blocking "objectionable" material, usually with technology bought from US firms. China is far and away the world champion. But it's felt the heat of competition in recent years. Each country in this far from complete list has its own style and tactics but they all have one purpose, to keep ahead of the game.

OVERALL WINNER : CHINA

The Chinese Communist Party (CCP) and the state have deployed huge human and financial resources to prevent the emergence of genuine freedom of expression online. News websites have been put under the editorial supervision of propaganda bodies at national and local level. With 48 cyber-dissidents behind bars, China systematically cracks down on bloggers. The government wants to keep control of news and information and censors the Net through a subtle mix of filtering and dissuasion. Several billion dollars have reportedly already been spent on censorship online. Since the summer 2007, two "cyber-police officers" appear on the screen of computers in cyber-cafes to warn Internet-users that they are being watched. The country is on its way to becoming the biggest Internet sector market in the world, ahead of the United States, and attracts more and more foreign companies, some of whom are ready to censor their networks.

BEST CRACKDOWN : IRAN

Internet is playing an ever greater part in Iranian society, which is strongly displeasing to President Mahmud Ahmadinejad who cannot bear to see his policies given a rough ride. The government has therefore equipped itself with a legal means of Web censorship. From 2006 onwards, all websites have had to register with the authorities and access providers have to ensure that "banned" content is not published by their servers. Photo-sharing site FlickR and video-sharing YouTube are inaccessible because of

some items considered by the authorities to be "immoral". The Net however remains the vehicle of social expression and allows women, for example, to demand their rights. Online journalists who post articles on women's magazines are regularly brought before the Tehran court for questioning. The authorities in 2007 arrested a score of male and female bloggers because of their online activities.

BEST SUPPORTING ROLE : US COMPANY YAHOO!

Thanks to its co-operation, the Chinese authorities have been able to put four cyber-dissidents in prison. Shi Tao, a 37-year-old journalist on Dangdai Shang Bao (Contemporary Trade News) was sentenced to ten years in prison in 2005 for "illegally divulging state secrets abroad", on the basis of information supplied to the government by the US company. He was found guilty of having posted on foreign-based websites an internal memo sent to his paper by the authorities. It warned journalists of the danger of social destabilisation and risks linked to the return of certain dissidents on the 15 anniversary of the Tiananmen Square massacre. The US company is now facing two sets of legal proceedings over the help it gave to the authorities. During a hearing on the Shi Tao case before the US Congress, the company's president, Jerry Yang, publicly apologised for the "misunderstanding" which put the journalist in prison and said it had been decided to create a fund dedicated to helping the families of cyber-dissidents.

BEST NEWCOMER : ZIMBABWE

The Web is not sufficiently entrenched in the country for the government to operate mass censorship, however Internet-users are openly spied on by the government, which concentrates on email. The government in August 2007 adopted a law authorising surveillance of all communications, via telephone or electronic. A request can even be made "orally" in "urgent or exceptional circumstances". Posting an article online that is critical of the government is extremely risky for the author. Censorship is carried out by the national telecommunications company TelOne which is closely controlled by the government of President Robert Mugabe. The company can ask access providers to monitor online communications with a simple request. The text of the agreement also asks them to "take the necessary steps" to prevent the spread of illegal content on the Net.

BEST ORIGINAL SCREENPLAY : BURMA

From the end of August to mid-October 2007, Burma went through its biggest uprising since the 1988 student demonstrations, when a brutal crackdown left 3,000 dead. The monks rebelled against falling living standards for the Burmese, bringing thousands of demonstrators out on to the streets with them. Faced by this "saffron revolution" the government deliberately cut off the country so that no evidence could get out. Between 28 September and 16 October 2007, the two access providers cut their Internet connections on the orders of the military junta. During this two-week blackout, Internet was only accessible for a few hours a day and all cyber-cafés were closed. For the Burmese, the only way of getting news was via satellite television or foreign radio stations

BEST FILTERING : SAUDI ARABIA

Unlike China or Iran, the Saudi filters make it clear that the authorities censor the Web. Many websites dealing with social life are inaccessible. Nearly 400,000 Web pages are blocked in the kingdom because of their "immoral" content, linked for example to homosexuality or women's rights. A commission is also to produce quality labels to "protect Saudi society" from this type of content. It was even decided to strengthen the law to fight terrorism, fraud, pornography, defamation or violation of religious values. Blogger **Fouad al-Farhan** was arrested and taken to prison in Jeddah on 10 December 2007 for having posted a commentary on the advantages and disadvantages of being Muslim.

King Abdallah Ben Abdel Aziz al-Saud

BEST CENSOR : VIETNAM

Internet penetration in Vietnam is higher than in China. From 2001, all Internet-users on the Vietnamese network are responsible for the content which they create, distribute or archive. Access providers received an order in 2006 to install software allowing them to keep their customers' details for one year. Filtering of political content is the responsibility of the interior ministry. The state is a shareholder in all access providers and can therefore easily keep them under control.

BEST SET : CUBA

Since Reporters Without Borders' escapade on this dream island in 2006, access to the Internet has worsened still further. There is only one remaining cyber-café left open in the centre of Havana. Cubans mostly have to use an Intranet (messaging, navigator and news) because access to the international network is very expensive. The government has no hesitation in silencing the most critical voices. Private Internet connections are considered to be illegal and an Internet-user can be sentenced to five years in prison for not respecting this rule. But he can also be sentenced to 20 years in prison for posting a "counter-revolutionary" article on foreign websites.

Clothilde Le Coz is head of the Internet Freedom desk at Reporters Without Borders

REPORTERS WITHOUT BORDERS
International Secretariat
47,rue Vivienne, 75002 Paris, France
Tél.: 33 1 4483-8484
Fax: 33 1 4523-1151

Website : http://www.rsf.org

Original graphic design and extra illustrations: Nuit de Chine

Support RSF's campaign on http://www.rsf.org

HANDBOOK OF **BLOGGERS** AND **CYBER-DISSIDENTS**

loggers cause anxiety. Governments are wary of these men and women, who post news without officially being journalists. Worse, they frequently raise sensitive issues which the media, now known as "traditional", dare not cover. In some countries, blogs have become a new source of news.

This updated version of the Handbook for bloggers and cyber-dissidents is available in French and English on the website http://www.rsf.org. The handbook offers advice and technical tips for the best way to launch a blog and how to get round online censorship. It includes an explanation of how to blog anonymously and contains articles by bloggers, particularly in Egypt and Burma.

REPORTERS WITHOUT BORDERS

www.rsf.org

REPORTERS WITHOUT BORDERS
FOR PRESS FREEDOM