Tech Tools

For activists

Privacy, anonymity and other stories

An introduction to this booklet

Sanjay and Magnus want to travel to a counter-mobilisation taking place around a summit in a large European city. Sanjay helps organise coaches to demos and sends inspiring emails to lots of people about using any means necessary to defeat capitalism. Magnus doesn't know about secure communications and fears that using email will get him into trouble, so only hears about the coach arrangements through personal meetings with friends. When it is time to go to the summit, the coach times are changed at the last minute. Magnus does not hear about them, so doesn't travel. Sanjay catches the coach, but is turned back at the border as he's on a list of 'known domestic extremists' whose emails have been monitored.

Effective political organising has always required good communication. Over the last two decades the information revolution has changed the way political activists communicate to an extent that was previously unimaginable. Alongside the new opportunities this has created, there also remains the age-old problem of how to get information to your political allies while maintaining confidentiality.

One of the oldest security techniques is to use an alias (or aliases) for your political persona. The idea is that very few people will know that your online nickname and email address are linked to your real name and address. In this way, if your alias is somehow incriminated, it will not be easy to discover the identity of the person behind the alias. You do not want to keep changing aliases, so you'll need email providers who will not (or cannot) disclose your personal details if they are pressured by the police.

Communicating securely is everyone's business. Even if your activism is super-fluffy, you can help make the internet safer for everyone by adopting good security practices. If only the people doing spiky things used these practices, they would attract attention just by doing so. Get into the habit of doing things securely before you really need to and you will be a thorn in the side of the surveillance state.

Next consider what you really need to transmit. Any information that could incriminate you or anyone else, or allow someone to undermine your intended action, should only be shared with people who need to know. So unlike planning for an open day at the allotment, you probably won't be CC-ing your local councillor about borrowing some bolt-cutters and a bulk order of Maalox.

Having decided who you want to talk to and about what, you need to consider three things:

- Synchronicity: do I want to send a message that can be picked up later or chat in real time?
- Authenticity: how will the person receiving the message know that it's genuinely from me?
- Privacy: how can I stop the message from being read by anyone other than the person/people I intend?

This table shows a selection of possible methods for secure electronic communication and how well they perform.	**Synchronous**	**Authenticated**	**Private**
Mobile or landline phone	✓	✓*	✗**
VoIP phone	✓	✓	✓***
Instant messaging using Off-The-Record	✓	✓	✓
Skype-to-Skype call or chat	✓	✓	✗
Email	✗	✗	✗
Facebook chat	✓	✗	✗
Crabgrass chat	✓	✓	✓
Signed Email	✗	✓	✗
Encrypted Email	✗	✗	✓
Signed, Encrypted Email	✗	✓	✓

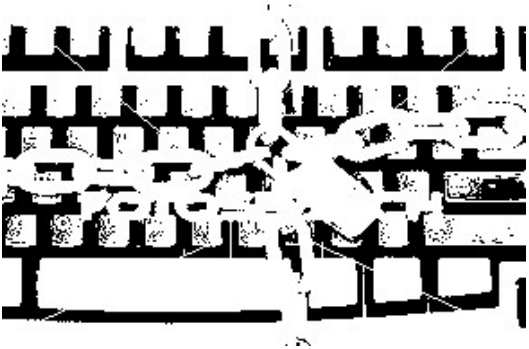
* A phone call can be authenticated if you recognise the voice of the caller.
** Phone calls can be intercepted.
*** VoIP calls can be routed through secure networks

As you can see, there are a few different approaches. The aim of this short booklet is to provide a cursory introduction to the effective use of technology for activism. It is not a step-by-step guide. It does not aim to explore all the possible options for you, but rather sets out simple ideas about good practice and how activists around the world can use and are using these techniques to advantage.

You might be wondering how to check the

authenticity of the sender of emails you receive, or perhaps you want to make sure that an email you send can only be read by who you desire. Then the chapter on securing your email is a good place to start. If you're looking to publish online, then we have two chapters on news publishing and uploading media, although first you might want to consider making your web browsing more anonymous as ever more legislation tries to restrict your freedom to surf; then the chapter on anonymous internet browsing is worth reading. One of the first principles on getting organised online is whether you can trust and rely on your chosen collaboration tool, social networking site, etc. Have a read of the organising online chapter to find out more about the benefits and pitfalls. Finally, to complete your arsenal of tools to wise up your activism, we have advice on clearing your Google cache and how to hide stuff on your computer so it can't be found.

We end with a some thoughts on the principles of the commons, free culture and how the free software movements are helping to produce software that is open and for the benefit of all.



Browsing the Internet Anonymously

Maria and her affinity group want to take action against a weapons factory near her home. She uses her home computer to do some research, including reading all of the websites that describe the factory and downloading some satellite images. After careful preparation, they get to the factory and spray some messages on the walls, then leave without getting caught. Next day, Maria has her door broken down by the police, who viciously demand that her house-mates tell them who uses which computer. Six months later, her affinity group are bringing food parcels into prison for her.

When we visit a website on the Internet we leave a trail of information behind us, both on our own computer and on the *server* (the remote computer that *hosts* the website): who we are, what we are looking at, when we looked at it and what pages we visited before and after the site we are currently looking at. When you visit a website, you leave a record of what is called your **IP (Internet Protocol)** address behind. This is unique to you and it is linked to the home address that the computer is being used at by your ISP (Internet Service Provider eg. BT or Virgin). The police or other agents can use this information to find out who has looked at what site and when. Your web browser is also likely to be disclosing all sorts of information about itself, and, by implication, about you too, without you knowing it.

Using an internet cafe or library may help. However, a lot of them require ID (library card, passport

or drivers licence) or may have CCTV.

Technical Approaches to using the Internet Anonymously

Here are a few broad categories to think about and pointers to further information.

- Can the network you are using be linked to you? If you use a public wifi hotspot, or if you buy a **pay-as-you-go 3G adapter** with cash, and then credit it with top-up cards bought with cash (check for CCTV in the shop), there is less chance of leaving a trail of evidence that leads to you.
- Your browser and operating system store a lot of information about you, probably without your knowledge. For this reason we recommend **using Firefox on a GNU/Linux system**, and following the instructions at http://tiny.booki.cc/?0ER8
- You can use a public Proxy, an easy way to make it more difficult to trace your Internet use. http://tiny.booki.cc/?proxy
- You can hide some information about your network location using a *proxy* (a computer that fetches web pages for you on your behalf), or better still a network of proxies and routers like the **TOR (The Onion Router)** project at https://www.torproject.org/ - for a great (and detailed) description of using TOR see http://tiny.booki.cc/?tor
- Another option is to use a **Linux live CD**, which allows you to run Linux straight off a CD (or USB stick) on any PC. All your activity is stored in the computer's memory, which as soon as it is rebooted leaves no trace behind. Check out http://puredyne.goto10.org as a great example.

- Using a Virtual Private network may be a possibility for you. **VPN (virtual private network)** and **tunneling** are techniques that allow you to encrypt the data connections between yourself and another computer
  http://tiny.booki.cc/?vpn
- There are no methods of security that are 100% reliable and they do not always work with all operating systems. It is a good thing to ask your techie friends about. There is a mailing list on aktivix where people may be able to help too: aktivix-discuss@lists.aktivix.org However be aware that it is open and publicly archived.

Organising Online

Jim is a union organiser and has formed a group on Facebook for his union that has attracted 5,000 members. The week before a large cross sector industrial action, he is shocked to find that Facebook has terminated his account and group. No explanation is given and he has no way to contact the thousands of people who had joined the group. His efforts have been wasted, the union's action scuppered.

Ways people Organise Online

There are several ways that people use the Internet to organise online. Some are listed below.

- Social Networking Sites
- Instant Messaging and Twitter
- Email and Email lists

Tools like Facebook, Google, Yahoo and many other Social Networking and email services have well documented security implications.

It is so common for the state to spy on people using these services that they have easy-to-use guidebooks to make their spying more efficient. Have a look at these leaked documents:

- facebook: http://dtto.net/docs/facebook-manual.pdf
- yahoo: http://dtto.net/docs/yahoo-guide.pdf
- myspace: http://dtto.net/docs/myspace-guide.pdf

Secure Tools for Organising Online

If you are concerned about the implications of organising online and do not want to exclude people who are careful about their privacy, then there are alternative you can use.

Crabgrass

Crabgrass is a Free Software web application run by an activist tech collective called RiseUp who will protect your security and anonymity as, like you, they are all activists working for radical grassroots change. The site that they provide at we.riseup.net uses a piece of software called “Crabgrass”, which is an activist equivalent of a social networking site. It allows you to create groups, work collaboratively on documents, be as private or as public as you want to be (and even have a different private and public profile), control who can and can’t be in the group based on whether you actually know them or not, and communicate securely by sending each other private or group messages.
For more information on Crabgrass see http://tiny.booki.cc/?crabgrass

Instant Messaging and Twitter

Corporate Instant Messaging (IM) tools include MSN

Messenger, Yahoo Messenger and Skype among others. These are all insecure. Twitter sells information about its users to third parties, but there is an open source alternative to it which lets you cross post to your Twitter account from it as well, http://identi.ca . But it is not very popular. You would be just as well to sign up to twitter and post anonymously by using Anonymous Web Browsing (see the chapter "Browsing the Internet Anonymously").

As far as IM goes, you can do live chat in a more secure way by using Crabgrass chat. When you are logged in to Crabgrass you can go to the Chat page (located on the main menu at the top). You can only chat with people that are members of groups that you have joined.

Internet Relay Chat (IRC) is a great old school way of chatting. Users install an IRC client or connect via a webpage and it is possible to chat in an encrypted way. A lot of techies, free culture and software enthusiasts and media activists use this technoloy. There is great help on setting up IRC. http://tiny.booki.cc/?secureirc.

Email and Email lists

See the chapter "Securing your email" for documentation on sending Email securely.

As far as Email lists go, some people simply maintain a list of contacts which you include in the to: or cc: field when you send an email. Or you can use a dedicated mailing list. These can handle large lists which you simply can’t do reliably manually.

The mailing list server allows people to subscribe to or unsubscribe from the list and handles security and privacy much better, so members of the list don’t automatically know the email addresses of all the other

members. The list server software can also create automatic archives which can be very useful.

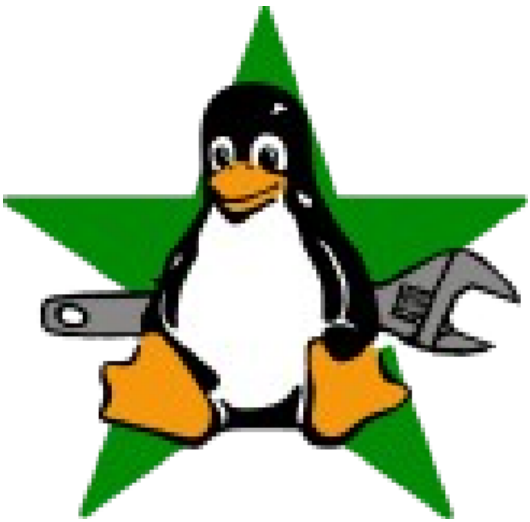
Lists provided by activist tech collectives are only as good as their weakest point – in other words, if just one person on your mailing list has an "@googlemail.com" address, you can't consider the list to be secure.

Consider the following points when creating lists:

- open or closed: can anyone subscribe or do subscriptions need to be approved?
- public or private: is the list to be advertised to the world, or is it run on a need to know basis?
- announce or discussion: is the list for receiving information only or for discussing something?
- moderated or not: are posts to the list to be moderated?

Collectives that provide mailing lists include the following:

- aktivix.org
- riseup.net
- psand.net



Securing your email

Arty got a new job and for a while continued to receive the emails of his predecessor. Soon enough, an email arrived that was addressed to the **key organisers of a high-profile grass roots activist movement***. As the person who sent the mail had placed everyone's email addresses in the To field, Arty now had a list of all the key organisers and a copy of the email. Neither the sender nor any of the recipients were aware of this; their trust was breached.*

Email has become one of the major forms of communication in the modern world, and because it is used so much by activists, there are a lot of email-related things to think about.

In the simple example above: when writing to a number of people use the *BCC* (blind carbon copy) field to send the email rather than *To* or *CC* fields. This ensures that no recipient knows who else has received the mail. Unless you have the permission of everyone on the your list to share their address with the other people, use BCC keep it secret. If you need the features of a mailing list, use one.

There are two key issues with a commercial webmail provider (such as Google, Hotmail or Hushmail).

1. They log usage and hand over your communications to the authorities on demand.
2. They reserve the right to terminate your account as they see fit, effectively terminating a digital identity that you may have invested a lot of time in.

So when using email for your activism, consider choosing a provider you can trust, such as Riseup, Aktivix or Inventati.

Activist mail hosting

These services are run by fellow activists who understand the need for privacy, anonymity and trust. You connect to them using a web page that runs over an encrypted connection. And unlike corporate providers, they will not give your emails over to the police without a warrant and a legal fight. If that happens, they will make it public if they can, so you (and the thousands of other activists on the same server) will know about it.

The secure email providers mentioned above also encrypt all messages sent between themselves, meaning that an email from an Aktivix user to a Riseup user is encrypted both as you compose it and when it travels between Aktivix and Riseup having been sent. In case it is not totally clear, those Gmail users on your mailing list are the weak link - consider putting some pressure on your activist friends, because their sloppy communications habits put you at risk.

Securing your own email

If you are concerned about privacy but not using a secure webmail service, or are communicating with someone who is not, or want an addition of level of personal security, you will want to encrypt your mail. Encryption is the process of taking a plain text message and converting into something that looks like gobbledygook, which at the other end can be decrypted and the original message restored.

The Free software tool of choice for this is called GPG, the GNU Privacy Guard. Most people, even well rounded techies, find GPG tricky to get their heads round. Give yourself time to look at this - and it may take some time - but it is worth it.

GPG encryption uses pairs numbers we refer to as

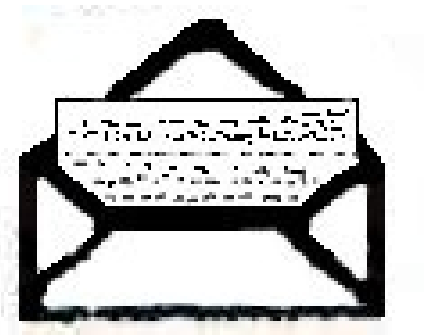
key pairs. GPG will help you generate your key pair, comprised of a public key and a private one. You need to give your public key to anyone you wish to have encrypted communication with.

Your private key you will keep absolutely secret and never ever reveal to anyone ever, as it is used to decrypt email sent to you. It is so very secret that it needs protecting with a *passphrase,* which is basically a very long password.

So could GPG have helped prevent the breach of trust mentioned above? GPG helps because by encrypting the email using the recipients' public keys, the sender can be assured that only the authorised recipients will be able to read it (privacy). Also the recipient can be assured of the identity of the sender (authenticity).

More information about setting up and using GPG with the popular Thunderbird email client can be found at these excellent articles

http://security.ngoinabox.org/thunderbird_main
http://www.freesoftwaremagazine.com/articles/secure_email



Publishing your News

Gabby was part of an affinity group doing animal rights actions. After each night time adventure she would write a brief communiqué and post it to a blog on blogger.com. Since the site supported RSS syndication, this news was easily pulled into an animal rights aggregation website and picked up by many other groups around the world. Gabby's blog was traced back to her and she served a 5 year prison sentence.

The internet has made it easy for everyone to publish news. Anyone can set up a blog or start twittering. With the ease of publishing, the internet is awash with info which makes reaching your audience more challenging. Making sure your content shows up in search engines like Google has become a science called Search Engine Optimisation (SEO). Using a blogging system or a well-known news site and tagging your content can help too.

Network internet services which let you share your news often keep a record of who is visiting and updating your news site. This causes security problems and legal problems as well.

Posting anonymously

Blog sites like wordpress.com and blogger.com and social networking sites like facebook keep a record of who uses their site. They do this by collecting the IP addresses.

There are two solutions for posting your news anonymously. You can use Tor to post anonymously on websites that log your IP addresses (see chapter "Organising Online") or you can post to websites that do not log your IP address.

Website and Blogs hosted on certain independent servers

There a number of servers that let you host your website or blog anonymously, like http://noblogs.org. They do not keep records of who is uploading what. In fact, they are actively trying to resist attempts by governments to impose laws on monitoring, as can be seen on the front page of the Aktivix website, http://aktivix.org/, and on the last page of this booklet.

Indymedia and other secure sites

Indymedia volunteers coordinate the production and sharing of news content often ignored by mainstream media. The global IMC network is based on openness and broad participation: all software is opensource, most lists are publicly archived, everybody can sign up to the wiki, log-on in chatrooms, or publish various newswire as long as it does not breach the guidelines.

Tagging your content

Tagging your content makes it much easier to find. If you use tags, your news can then be classified, better indexed by search engines, and via RSS feeds the content it can be pulled into other websites (aggregation).

RSS and aggregation

Syndication offers some potential for posting anonymously. RSS feeds are an agreed standard to allow different sites to pull in and republish content from other sites. You could publish your news anonymously on Indymedia - which uses tagging, and an RSS feed - to republish it onto your convenient (but insecure) wordpress.com site.

Uploading Media to the Internet

Nico made a short video of the London Naked Bike ride and uploaded it to YouTube. Because the title contained the word 'naked' there were plenty of people looking at it. Within a couple of days the video had been removed from YouTube without explanation, and correspondence established that there was no appeal process.

This does not mean you should not use YouTube and other file sharing sites. But there are other free (as in freedom) hosting sites such as Indymedia, Politube, EngageMedia among others.

YouTube has vast potential audiences but that potential doesn't necessarily translate into actual audience. There are a lot of videos on YouTube that are viewed by hardly anyone. Often it takes quite a bit of effort and networking to get people to view your content. So you might be able to build an audience in different ways which do not rely on a network service that could suspend your account at any time.

In any case, quality may be better than quantity. When producing any media you should always ask yourself who your audience is and create a strategy that reflects this.

Editing and Encoding video

The Message in a Box project included downloads and guides for tools to help you create, publish and play your video. In addition, there is also a selection of video tools available for advanced users.
http://tiny.booki.cc/?videotools

Features of Video Uploading

There are different levels of independence and features that you may want from a video sharing service.

- Can you edit and remove your content completely?
- What licence are you releasing your video under?
- Can you view video in a streaming player, download a file and embed this player into other websites?
- What formats can users download your video file in? Do you want to support open formats?
- Does the platform support RSS feeds that can be used in podcasts?
- Is it possible to post and view videos anonymously?

There are quite a few corporate 'Web 2.0' services that offer a lot of functionality and provide a high degree of usability. However, none of the commercial services can be relied upon to offer anonymous posting and/or viewing.

Running your own Video sharing site

There are a number of Free/Libre/Open Source Software (FLOSS) web Content Management Systems (CMS) that offer specialised video functionality - such as Plumi http://plumi.org/ and various video-specific Drupal and Wordpress modules. There is a network of groups and individuals called Transmission, who share knowledge

about video CMSs and would be happy to help on their email list. http://transmission.cc

Video sharing services

Indymedia.org.uk allows you to upload video files anonymously but you do not get a streaming video player or an RSS feed; however streaming video player and RSS feeds are being worked on in various indymedia sites in the UK.

Archive.org contains thousands of digital movies ranging from classic full-length films, to daily alternative news broadcasts. All these movies are available for download, often in very high resolution, and are freely licensed. You can embed the video into other websites, but you ca not create an RSS podcast there. They support open formats like Ogg video. You cannot upload content anonymously.

The WITNESS Hub is an online video community for human rights where you can upload, watch and share human rights-related videos, images and audio files in a variety of formats. WITNESS also offers training, support and resources, plus RSS feeds and a large and growing archive. It is available in English, French and Spanish. The Hub also has a **toolkit section** that features video animations about how to incorporate video into your campaign work and best practice when filming and distributing your video.

Other services: There are links to the above sites and good overview of choosing a video platform and preparing video for the internet on the Message in a Box toolkit. http://tiny.booki.cc/?videoplatforms.

Hiding Stuff on your Computer

Noralee publishes an underground newsletter, "Knitting for Anarchy!". One day one of the articles causes quite a stir, being implicated in provoking a series of assaults using crochet hooks against politicians. The police confiscate Noralee's computer, find out who wrote the piece and arrests the author. Noralee wishes that the police could not have read her confidential documents.

There are three basic solutions to hide files - physical hiding, encryption and misdirection. Physical hiding would mean using a portable medium such a USB key and keeping it in a secure location, only to be brought out for editing. This has limited scope - and it is a pain.

Encryption does not require any physical movement of media. Encrypted data cannot be read directly and must go through some kind of unlocking in order to be useful. This allows only a select group of people or computer systems to be given access to the data; only those with the key will be let in.

The third solution, which can be used in conjunction with the others, relies on what stage-magicians call "misdirection." This means placing the material of interest in a place in a block device (hard disk, etc.), a filesystem, or within another file or container, where nobody would think to look; or if they did look there, would not be able to prove that it was really anything other than random information. This last case is an example of plausible deniability.

For Mac OS you can visit: http://tiny.booki.cc/?v9eT

Do not use the passworded folders system on Microsoft Windows, as it offers you little real protection. Check this page for Windows: http://tiny.booki.cc/?NtGz

The latest versions of Ubuntu offer the user the chance to encrypt the home directory (where you put your files) during the installation process.

Important

However - it is important to be aware of the fact that on all modern operating systems Linux, Windows, OSX etc, there is a feature called virtual memory, which basically allows programs running on your computer to use a piece of your hard drive in a similar fashion to how they use RAM. This kicks in when more memory is required than is provided for by the RAM chips in your computer. On windows this information is stored in the pagefile on your hard drive and on Linux/BSD/OSX etc. it is stored on the swap partition.

To prevent people from reading the information that is left there you must also encrypt the pagefile or swap space.

A simplest solution to this is to encrypt your whole hard drive. Various Linux versions have this feature built into their installers and there are plenty of wiki's out there on how to do this. If you're stuck with using Windows, using TrueCrypt for encryption of your whole hard drive is probably the way to go.

After encrypting your hard drive and swap/pagefile you can obscure it too. When using some Free Software operating systems; for example Ubuntu, you can create a space on your computer like the home directory were you can store files that can only be accessed when a password is entered, when a particular USB key is present in the system, or any number of criteria are met.

It is important to remember that, like with securing your house, no system is fool-proof. As new systems are developed to secure doors, other systems are developed too in order to break them. The key issue is to be aware of the risks, the ways available to protect yourself from those risks, and the trouble you are prepared to go into in order to do that.

For example, if your computer/laptop has been bugged or compromised in some way, it doesn't matter how good your cryptography is if your keystrokes are being recorded. Using an operating system where installing bots that do that is more difficult is a useful first step towards enhanced security.

How to get pages removed from Google Cache

Scenario

A story on Indymedia reported part of a campaign against the deportation of an asylum seeker who was later granted refugee status. The story's central figure has a distinctive name and did not want his immigration history to remain public. Indymedia was contacted by his friends from a local No Borders group who had supported his campaign, saying that he wanted to 'put his past behind him'. All personal contact details had already been removed from the story and it was later hidden. However, one month later, Indymedia was asked why the story still appeared when the subject googled his own name. The subject's friends had already been advised to get the content removed from Google cache but did not know how.

Google provides at least 3 different ways for cache content to be manipulated:

1. a process for webmasters, which requires a validation process that might compromise the privacy of the administrator
2. a process for 'data subjects' (people about whom information is stored)
3. a faster process for people who may become victims of identity theft

These instructions relate to 2.

Before you begin

It only makes sense to ask Google to refresh their cache if a particular URL's content has been changed since the last time it was crawled. So, make sure that the cached version of the page is different from the directly accessed page.

Google stores all kinds of information about people, so for your own privacy you may want to:

- perform all of the following through the tor network
- create a disposable email account
- ensure your browser has no Google cookies stored
- temporarily change your browser's user agent string (e.g. in Firefox you can use the Tamper Data or Switch User Agent add-ons)

Create a disposable Google account

1. Start at www.google.com/webmasters/tools/removals
2. Using the link at the bottom right of the page, create an account
3. Follow the steps to create an account using your disposable email address
4. Clear the 'stay signed in' and 'enable web history' tick-boxes
5. Verify your 'identity' using the link sent to your disposable email address

Fill in the forms

The verification link should take you back to the webpage removal request page. If it doesn't you can

initiate a new
request: https://www.google.com/webmasters/tools/removals?action=create&hl=en

1. Choose the first option in the list, “Information or image that appears in the Google search results.”
2. Click ‘next’
3. The second page allows you to specify whether the page has been **modified** or **removed.** Choose the former if personal information has been deleted from a page that still exists; choose the latter if the story has been ‘hidden’ (either unpublished or meta-tagged ‘noindex’.)
4. Click ‘next’

Modified pages

If personal information has been removed from a story, the next page requires that you enter the search terms that would lead someone to find that story. For example, if searching for ‘myunusualname’ is how people would find the cached story that’s had ‘myunusualname’ (and/or other personal information) removed from it, you need to specify the URL of the story that’s been modified (in the upper box) and the search term (‘myunusualname’) in the lower box.

Removed pages

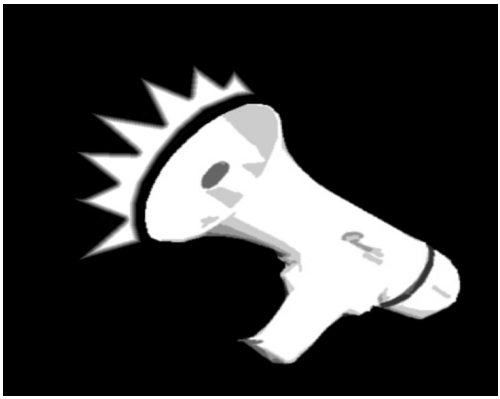
If a story has been ‘hidden’, the html output should include a meta-tag to exclude it from indices so all we need to do is ask Google to honour that by refreshing their cache and index. For pages that are availalbe using both "https" and "http", it is best to make the request for both URLs to be sure both caches are updated.

Finish

Logout and clear all Google cookies, form data and saved passwords from your browser. Google claim that these requests take 3-5 days to process, so do not expect instant results.

Free as in Freedom

Janet and Sammy are a pair of activists with a casual romantic involvement, who are doing community organizing around anti-racist issues. Janet installed a copy of Windows a few years ago on her computer, and no longer updates the anti-virus software. Her computer is hacked and put out of action by for-profit hackers using a Brazilian botnet that sends short-dick spam to all the email addresses on her address book. Before all this renders her unable to do any online political organising, Sammy receives one of the spam emails and recognises it as emanating from Janet's machine, and mistakenly believes that Janet is telling the whole world their secret.



What is Free Software?

Computer programmers in the Free Software community have collectively spent millions upon millions of hours of their free time writing virus-free, highly secure software that respects your privacy. You may have already seen or used some of this software: Firefox, OpenOffice, and GNU/Linux operating systems such as Ubuntu are used by hundreds of millions of people worldwide.

Is *Open Source* software the same? The term 'Open Source' was coined to make Free Software more acceptable to the business community by avoiding referring to the movement's foundations in the politics of freedom.

The Free Software we are talking about here is free to run, you are positively encouraged to see how it works and change it to your own needs and you are free to redistribute it. All these rights are protected in the software's license, most commonly the GPL (General Public License). If you change or improve free software and then re-distribute it, you must release your changes under the same license in order that everyone else can benefit from them. This beautiful way of licensing means that with each enhancement our pool of free programs grows in quality and features, and belongs to all of us for ever in freedom. It also means that for every techie that can fix a bug in the corporate software world, there are tens if not hundreds in the free software community.

Virus outbreaks in the context of GNU/Linux are so unheard of, and so quickly fixed when they have happened, that they have become the stuff of legend. In general GNU/Linux is considered by programmers to be more secure than Windows.

Ethics and Politics of Free Software

It is important to distinguish between software that is free in terms of cash and that which is designed with freedom in mind. Software might cost you nothing to download and use, but might still impinge upon your liberty.

Free Software is written by people who see software as inherently political. They are coding for an ethical purpose, namely to ensure that people retain self-managed control over their own information infrastructure. In contrast, large software corporations are concerned primarily with profit and with locking you into using their products.

Link to the four freedoms: http://tiny.booki.cc/?9he7
Link to wikipedia: http://tiny.booki.cc/?cbQt

Free Network Services

Abstinence from software services may be a naive and losing strategy in both the short and long term. Instead, we can both work on decentralization as well as attempt to build services that respect users' autonomy:

> "*Going places I don't individually control — restaurants, museums, retail stores, public parks — enriches my life immeasurably. A definition of "freedom" where I couldn't leave my own house because it was the only space I had absolute control over would not feel very free to me at all. At the same time, I think there are some places I just don't want to go — my freedom and physical well-being wouldn't be protected or respected there.*
> "*Similarly, I think that using network services makes my computing life fuller and more satisfying. Can we make working on network services more like visiting a friends' house than like being locked in a jail?* "*Time will tell whether we can craft a*

> *culture around Free Network Services that is respectful of users' autonomy, such that we can use other computers with some measure of confidence*."

Evan Prodromou, "RMS on Cloud Computing: "Stupidity"", CC BY-SA, http://autonomo.us/2008/09/rms-on-cloud-computing-stupidity

Further Info

This short booklet was always going to have to strike a difficult balance between the vast amount of information out there on the topic of online security, and the need to make it accessible enough to be understood by humans. Whilst we have tried to condense and simplify all of the information we could into this booklet, it is by no means a comprehensive or in depth guide. Instead we hope it will give the reader an introduction to good practice for activists whilst using the internet, and a desire to find out more. Here is a list of further reading for those who wish to delve a little deeper. Whilst this list is by no means exhaustive, it should help to point you in the right direction.

General How To's

docs.indymedia.org

A vast wealth of knowledge accrued over 10 years of providing a secure alternative to the mainstream media. Amongst the highlights on this site, you can find out how you can set up your own local Indymedia centre, as well as there being documents available on many aspects of running secure websites/groups/communications network. https://docs.indymedia.org/

wiki.aktivix.org

Aktivix is a UK based radical tech collective and their wiki contains articles on many aspects of internet security along with practical advice on a range of subjects and a space for groups documentation.
https://en.wiki.aktivix.org

flossmanuals.net

FLOSS Manuals is a collection of manuals about free and open source software together with the tools used to create them and the community that uses those tools. There are manuals that explain how to install and use a range of free and open source softwares, about how to do things (like design) with open source software, and manuals about free culture services that use or support free software and formats.
http://en.flossmanuals.net

tacticaltech.org

Tactical Tech is an international NGO helping human rights advocates use information, communications and digital technologies to maximise the impact of their advocacy work.

http://tacticaltech.org

howtoforge.com

HowtoForge provides user-friendly Linux tutorials about almost every topic.

http://howtoforge.com

Alternatives to corporate providers:

- **news:**
  http://www.indymedia.org.uk/
  http://www.schnews.org.uk
  http://www.theregister.co.uk/
  (Alternative to: BBC news, The Guardian, CNN)
- **email:**
  https://mail.riseup.net/
  https://en.wiki.aktivix.org/Activix:EmailAndLists
  (Alternative to: hotmail, gmail, yahoo, hushmail etc)
- **wiki, forum, chat, and much more:**
  https://we.riseup.net/
  (Alternative to: Facebook, Myspace, Bebo etc)
- **blogs:**
  http://blogsport.eu/
  http://noblogs.org/
  (Alternative to: Wordpress, Blogspot etc)

note: whilst not strictly a blog, many of the new breed of Indymedia sites such as london.indymedia.org and northern-indymedia.org now implement a “Groups” feature which means all members of your collective can publish content together and have your own mini site in the time it takes to create an account.

- ***search engines:***
  http://scroogle.org/
  (Alternative to Google that doesn’t log your personal details)

The author: HacktionLab

HacktionLab is a regular convergence space where activists interested and/or working in the areas of alternative media, renewable energy, on-line video distribution, free software or any other form of activism that utilises technology, can get together and plan how to better harness the technology (or not) to support grass roots social movements.

Visit our web site to find out more about HacktionLab-run events and gatherings, including our summer rural gathering, BarnCamp, which takes place in June in the Wye Valley.

HacktionLab is self-funded and the printing of this book was paid for by contributions from members. If you have a copy of this book in your hands and you find it useful, we would welcome a donation from you. We suggest one pound per booklet.

You can find out about way to donate to HacktionLab by visiting http://hacktivista.net/donate

Statement on Data Retention 2008

We want to stop Data Retention of the type that is being imposed on us by the E.U. Directive 2006/24/EC because it is a preemptive surveillance of communication structures:

Imagine the postal services kept a record of everyone who sent a mail to you. When. Who. How. Where. This is exactly what is happening now with your email, your phone calls and other electronic communications.

We as providers are forced to store YOUR communication metadata. This is forcing us to work as outsourced police forces. We do not want this. We will pour as much sand into this machine of suspicion as we possibly can. And we encourage everyone else to do the same! Do not support this attack on privacy!

We will continue to fight against Data Retention in any way possible and we will support each other in our different efforts to fight it.

Signed:

aktivix.org	hacklab.dk	open-web.fr
all2all.be	herbesfolles.org	poivron.org
alterezo.be	immerda.ch	puscii.nl
blacksec.org	koumbit.org	rezo.net
blogxpopuli.org	lautre.net	riseup.net
boum.org	linefeed.org	samizdat.net
cassiopea.org	manitu.de	sindominio.net
crackedwillow.net	marsupi.mine.nu	so36.net
domainepublic.net	moviments.net	squat.net
effraie.org	mutins.net	systemausfall.org
espace4you.org	nadir.org	systemli.org
free.de	no-log.org	tachanka.org
globenet.org	nodo50.org	toile-libre.org