Table of Contents

Table of Contents

Surveillance and privacy on the internet; some observations and some tactical responses.

aland@burngreave.net

gpg key 0x085CA9E8 Available on public keyservers

Schneier on privacy

"Privacy protects us from abuses by those in power, even if we're doing nothing wrong at the time of surveillance.

We do nothing wrong when we make love or go to the bathroom. We are not deliberately hiding anything when we seek out private places for reflection or conversation. We keep private journals, sing in the privacy of the shower, and write letters to secret lovers and then burn them. Privacy is a basic human need.

[...]

For if we are observed in all matters, we are constantly under threat of correction, judgment, criticism, even plagiarism of our own uniqueness. We become children, fettered under watchful eyes, constantly fearful that -- either now or in the uncertain future -- patterns we leave behind will be brought back to implicate us, by whatever authority has now become focused upon our once-private and innocent acts. We lose our individuality, because everything we do is observable and recordable.

[...]

This is the loss of freedom we face when our privacy is taken from us. This is life in former East Germany, or life in Saddam Hussein's Iraq. And it's our future as we allow an ever-intrusive eye into our personal, private lives.

Too many wrongly characterize the debate as "security versus privacy." The real choice is liberty versus control. Tyranny, whether it arises under threat of foreign physical attack or under constant domestic authoritative scrutiny, is still tyranny. Liberty requires security without intrusion, security plus privacy. Widespread police surveillance is the very definition of a police state. And that's why we should champion privacy even when we have nothing to hide." - Bruce Schneier - http://www.schneier.com/essay-114.html

Eric Schmidt on Privacy

"I think judgment matters. If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place. If you really need that kind of privacy, the reality is that search engines -- including Google -- do retain this information for some time and it's important, for example, that we are all subject in the United States to the Patriot Act and it is possible that all that information could be made available to the authorities." - Eric Schmidt CEO Google -
http://gawker.com/5419271/google-ceo-secrets-are-for-filthy-people

Things can change

"Of the 140,000 Jews that had lived in the Netherlands prior to 1940, only 30,000 survived the war. This high death toll had a number of reasons. One was the excellent state of Dutch civil records: the Dutch state, prior to the war, had recorded substantial information on every Dutch national. This allowed the Nazi regime to easily determine who was Jewish (whether fully or partly of Jewish ancestry) simply by accessing the data."

http://en.wikipedia.org/wiki/History_of_the_Netherlands_%281939%E2%80%931945%29#High_Jewish_death_toll

Recent Computer Security cases

- Indymedia Server Seizure - 2004 - not encrypted
- Bristol Indymedia Server Seizure - not encrypted
- Austistici/Inventati - http://www.autistici.org/ai/crackdown/comunicato_en_210605.html - not encrypted
- SHAC - google docs in browser cache, RIPA used
- indymedia Server seizure 2009 - Encryption - Serious Crime Act (incitement) - RIPA
- Sean Kirtley - Sequani - Coordinating actions on websites - Not encrypted
- M1 Widening - Sheffield - PC Seizure
- Liquid Bomb Terrorists - Email interception - Yahoo feeds to NSA
  http://www.schneier.com/blog/archives/2009/09/nsa_intercepts.htm
  http://www.wired.com/threatlevel/2009/09/nsa-email/
- Abbeydale road terorist - RIPA -
  http://b2fxxx.blogspot.com/2008/10/court-of-appeal-rules-no-defence-for.html

general corporatisation/centralisation of the internet protocols

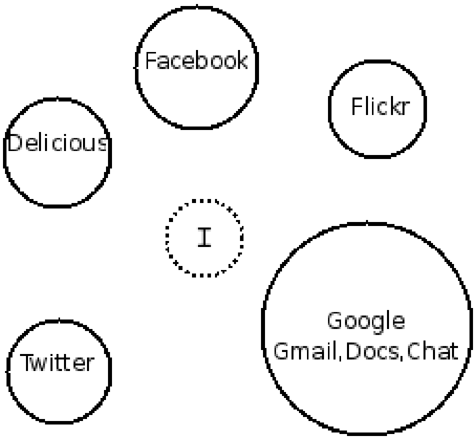
Facebook, Myspace, Hotmail, Google, Yahoo, Twitter

Where as the internet was designed as a p2p network, (my email server contacts your server, if the path between is blocked we can route around), now interactions are channelled through centralised paths in homogenous sites.

Provide free services - useful - email,search,social networking, blogs, storage...

monetise free services by intercepting communications,aggregating, analysing and reselling them

Current model is flawed - identity and data is owned by commercial entities, not by you



Lawful spying guides

All the large web corporations have well defined protocols to interface with law enforcement and govermental agencies

These protocols have been leaked to 3rd party's and are available on the internet.

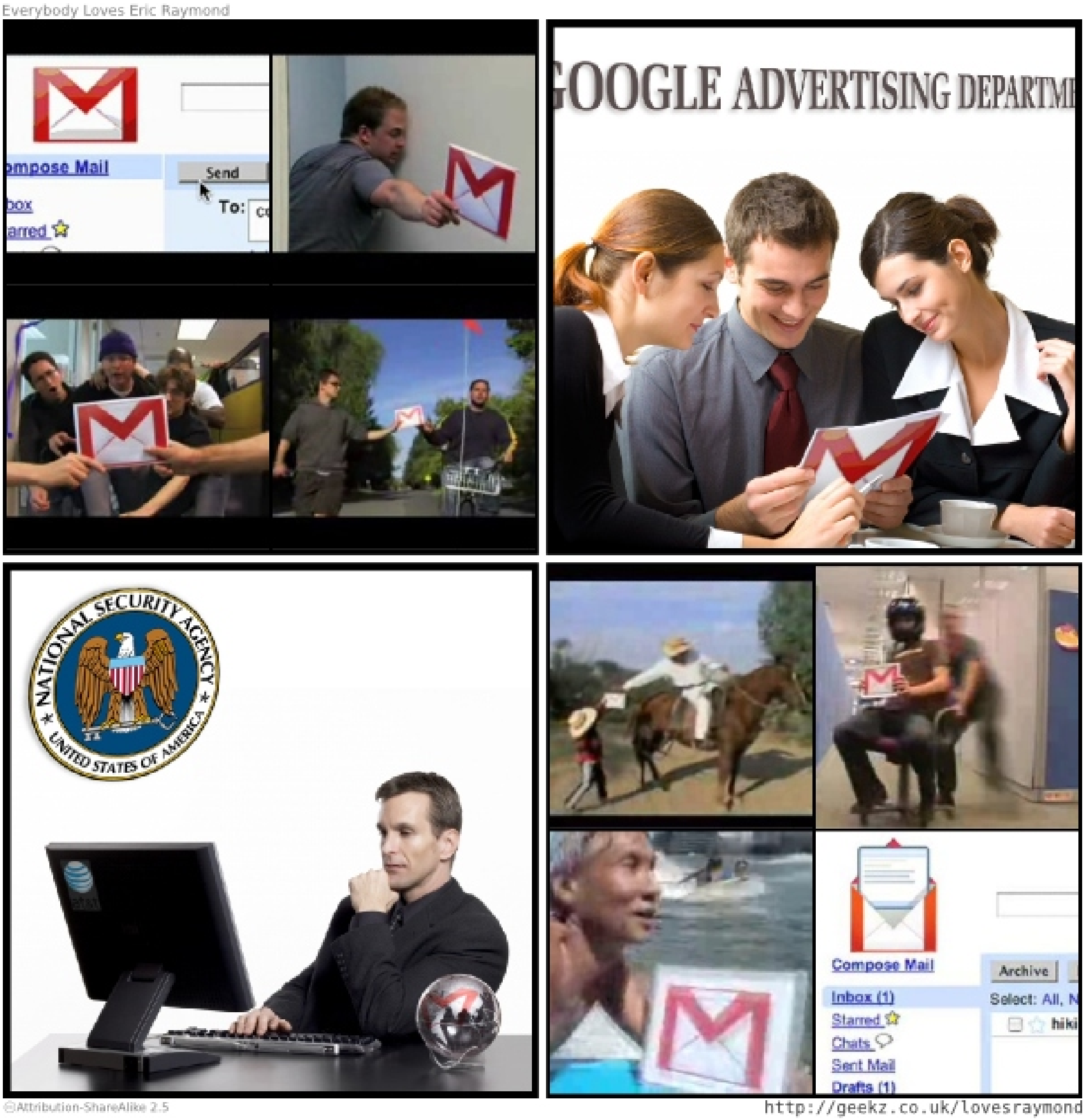
A good source for these is at http://cryptome.org/isp-spy/online-spying.htm

example of these

- "MySpace also collects and stores certain information that, depending on the information at issue, may be available only to MySpace (IP logs), only to the user and MySpace (private messages) "
- "All registration data is provided by the user EXCEPT for the Registered from IP Address. Occasionally the "Registered from IP Address" field may blank for some accounts. In this situation the user's IP address was not captured by Microsoft's systems during the registration process. Microsoft retains e-mail account registration records for the life of the account. For free MSN Hotmail and free Windows Live Hotmail accounts, the e-mail content is typically deleted after 60 days of inactivity. Then if the user does not reactivate their account, the free MSN Hotmail and free Windows Live Hotmail account will become inactive after a period of time.
- For Yahoo! Chat and all forms of Messenger, Yahoo! has log information regarding the use of the services. Yahoo! maintains a 'Friends List' for users of Yahoo! Messenger and can determine from its logs the time and date that a user logged into Messenger or Chat (in the prior 45-60 days) and the IP address used. Yahoo! also can retrieve from its Chat and Messenger logs the names of the chat rooms that the user accessed and the Yahoo! IDs of the other people with whom a user communicated through Messenger during the prior 45-60 days. In order to search these logs, a Yahoo! ID and a specific time frame, preferably no more than three days, must be provided.

What happens when you send a gmail - deleted scenes

from http://geekz.co.uk/lovesraymond/archive/gmail-behind-the-scenes-deleted-scenes



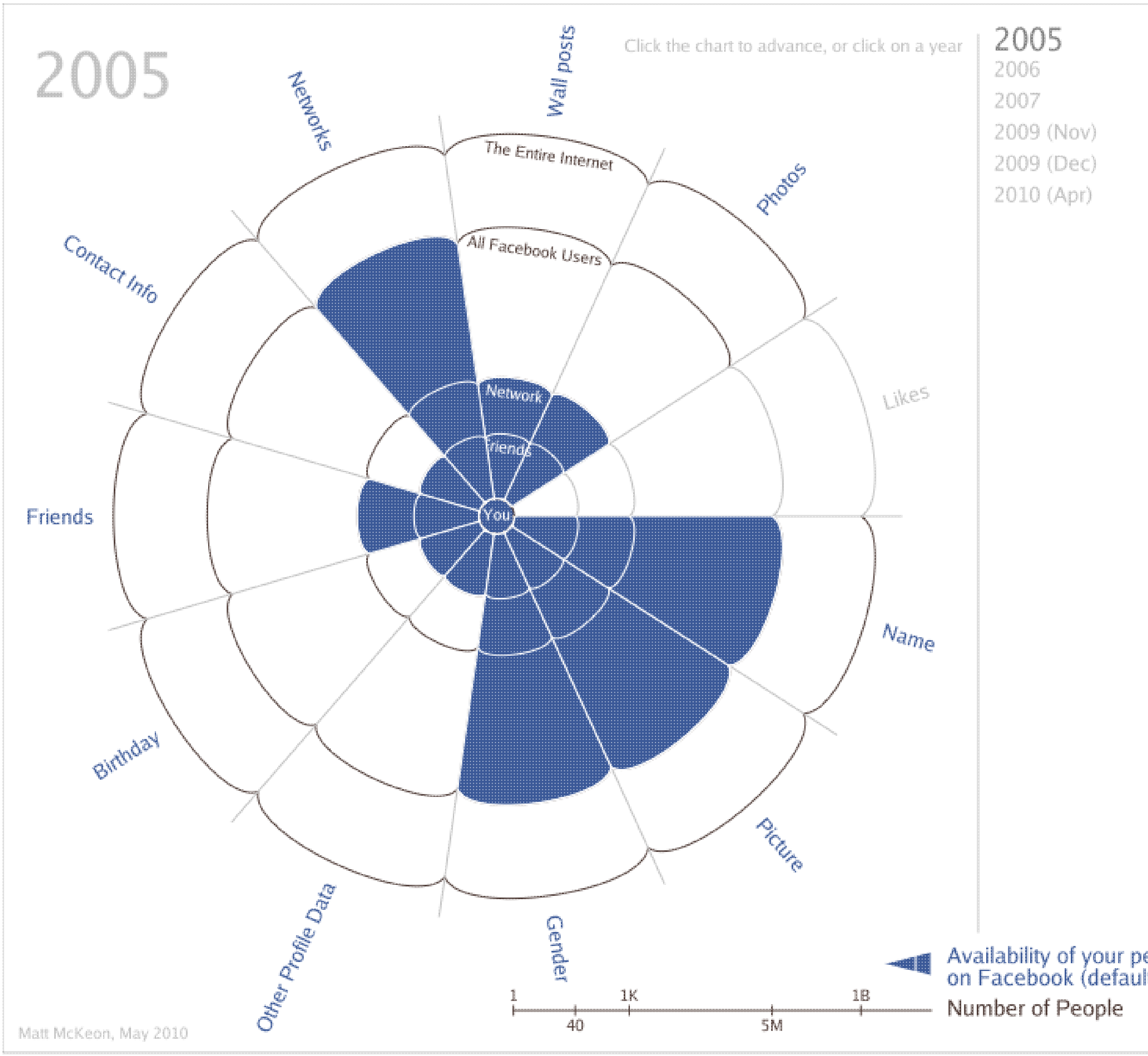
problems with facebook

- Police spying protocol - as with other providers
- Group messaging limits (was 1500 now 5000)
- Groups and accounts can mysteriously disappear - Indian Pink panty campaign, and Strawberry Fayre campaign http://www.whatdotheyknow.com/request/did_police_silence_strawberry_fa

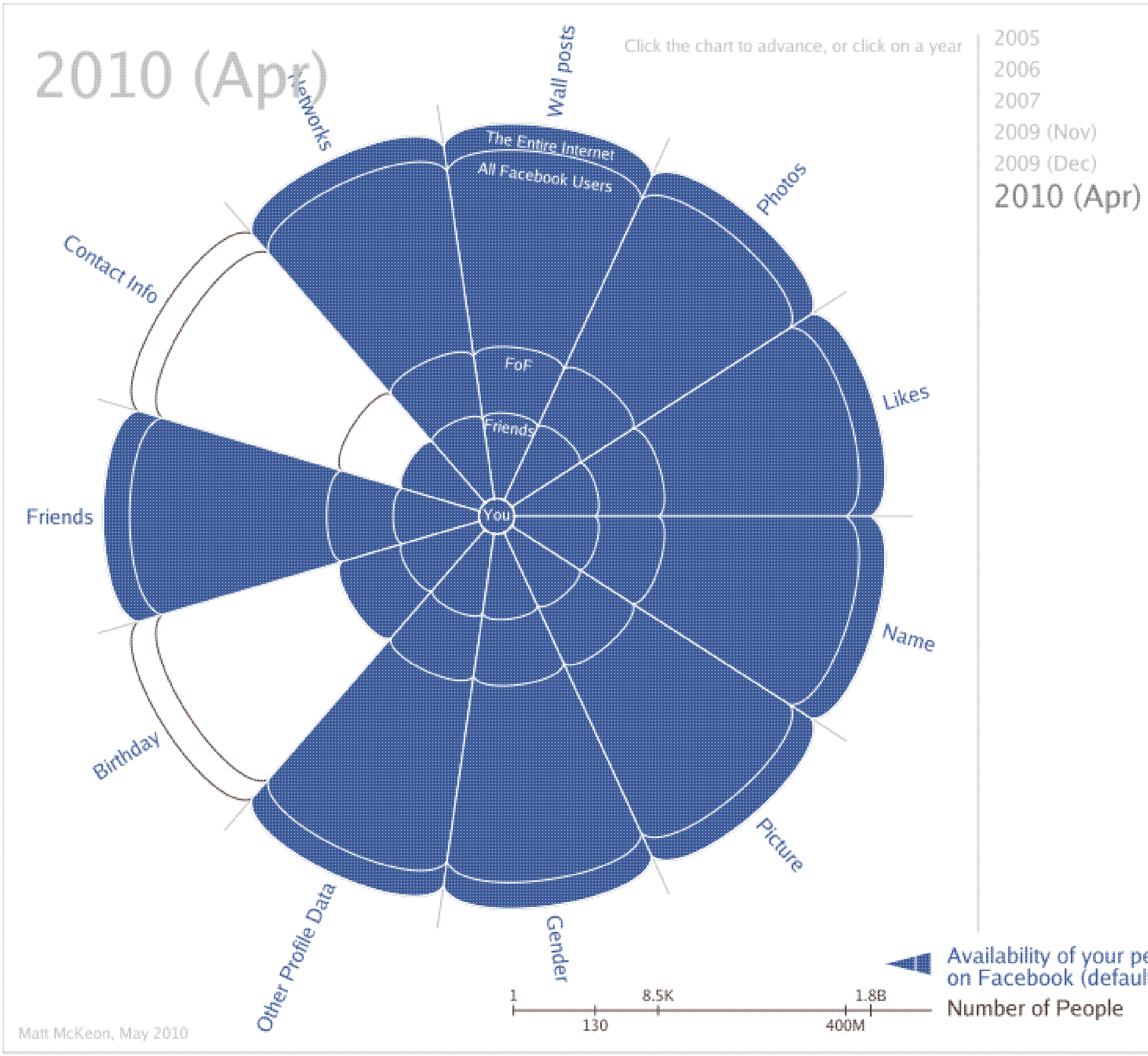
problems with facebook

changes in default privacy in facebook

2005



2010



source http://mattmckeon.com/facebook-privacy/

Who owns facebook

three board members on Facebook

- Mark Zuckerberg - inventor
- Peter Thiel
- Jim Breyer

Peter Thiel - right wing American Neo conservative, member of thevanguardist.org

Jim Breyer - linked to In-Q-Tel. http://www.iqt.org/ Owned by CIA

In-Q-Tel recently purchased stake in twitter search software

Facebook - owned by right wing capitalists who want to commodify every aspect of human relationships, and government spooks

http://www.wired.com/dangerroom/2009/10/exclusive-us-spies-buy-stake-in-twitter-blog-monitoring-firm/

http://www.guardian.co.uk/technology/2008/jan/14/facebook

Do you trust your ISP ?

How do you know they are not interfering with your data ?

wikipedia and IWF

"On 5 December 2008, the Internet Watch Foundation (IWF), a British watchdog group, blacklisted content on the English version of the online encyclopaedia Wikipedia related to the Scorpions' 1976 studio album Virgin Killer"

All UK access to wikipedia suddenly appeared to come from a 2 IP addresses. Because of the way that wikipedia manages access to edit pages (to protect them from vandalism) anonymous editing of wikipedia pages from the UK became impossible. The IWF reversed their blacklisting of the page on 9 December 2008.

http://en.wikipedia.org/wiki/Wikipedia:Administrators%27_noticeboard/2008_IWF_action
http://en.wikipedia.org/wiki/Internet_Watch_Foundation_and_Wikipedia

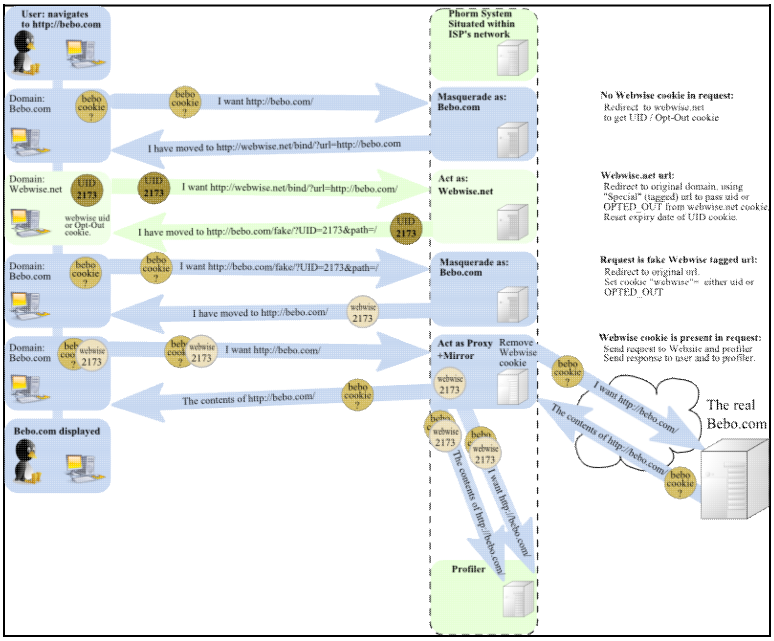
Phorm

Proposed to be used by some UK ISP's. Intercepts all web requests, and passes your browsing history to 3rd parties.

Trialled secretly by BT in 2007 and only discovered by accident.
http://www.theregister.co.uk/2008/02/27/bt_phorm_121media_summer_2007/

Temporarily used by other large ISP's (virgin media, talk talk), and web site (guardian.co.uk)

BT investigated by CPS, no charges brought


User: navigates to http://bebo.com
Phorm System Situated within ISP's network
Domain: Bebo.com
bebo cookie ?
I want http://bebo.com/
Masquerade as: Bebo.com
I have moved to http://webwise.net/bind/?url=http://bebo.com
Domain: Webwise.net
UID 2173
I want http://webwise.net/bind/?url=http://bebo.com/
Act as: Webwise.net
webwise uid or Opt-Out cookie.
I have moved to http://bebo.com/fake/?UID=2173&path=/
Domain: Bebo.com
bebo cookie ?
I want http://bebo.com/fake/?UID=2173&path=/
Masquerade as: Bebo.com
I have moved to http://bebo.com/
webwise 2173
Domain: Bebo.com
I want http://bebo.com/
Act as Proxy +Mirror
Remove Webwise cookie
The contents of http://bebo.com/
Bebo.com displayed
The contents of http://bebo.com/
I want http://bebo.com/
Profiler
The real Bebo.com

No Webwise cookie in request:
Redirect to webwise.net
to get UID / Opt-Out cookie

Webwise.net url:
Redirect to original domain, using
"Special" (tagged) url to pass uid or
OPTED_OUT from webwise.net cookie.
Reset expiry date of UID cookie.

Request is fake Webwise tagged url:
Redirect to original url.
Set cookie "webwise"= either uid or
OPTED_OUT

Webwise cookie is present in request:
Send request to Website and profiler
Send response to user and to profiler.

VirginMedia starts deep packet inspection

"Virgin Media will trial deep packet inspection technology to measure the level of illegal filesharing on its network, but plans not to tell the customers whose traffic will be examined"

The trial will cover about 40 per cent of Virgin Media's network, a spokesman said, but those involved will not be informed. "It would be counter-productive because it doesn't affect customers directly," he said.

- http://www.theregister.co.uk/2009/11/26/virgin_media_detica/

Legal threats to internet users

March 2007 - June 2009

"Two law firms have been sending out letter claiming that the recipients have illegally made available, on filesharing networks, certain computer games, music and even pornographic films. An estimated 25,000+ letters have been sent with many more sure to follow. Many agencies who can help may have received one or two letters from, or had meetings with, worried recipients. They will have seen documents directed at individuals but may have scant information on the scale of the operation.

Data is provided by two private monitoring companies: Digiprotect and Logistep based, respectively, in Germany and Switzerland. They harvest IP addresses (unique internet addresses which identify a connection) from filesharing networks. The solicitors, instructed by the game, music and movie publishing companies, then use a Norwich Pharmacal order (NPO) [10] to get subscriber data for the IP addresses from the internet service providers (ISPs)."

http://beingthreatened.yolasite.com

Interception modernisation project

Mastering the Internet

May 2009

http://www.timesonline.co.uk/tol/news/politics/article6211101.ece

"GCHQ, the government's eavesdropping centre, is developing classified technology to intercept and monitor all e-mails, website visits and social networking sessions in Britain. The agency will also be able to track telephone calls made over the internet, as well as all phone calls to land lines and mobiles.

The Â£1 billion snooping project - called Mastering the Internet (MTI) - will rely on thousands of "black box" probes being covertly inserted across online infrastructure. "

policeware

heard of spyware, malware, ... now there is policeware

- FBI magic lantern - Keystroke logging software, Undetectable to some AV software. see http://en.wikipedia.org/wiki/Magic_Lantern_%28software%29
- Microsoft Computer Forensic Evidence Extractor http://en.wikipedia.org/wiki/Computer_Online_Forensic_Evidence_Extractor

Defences ...?

radical tech collectives

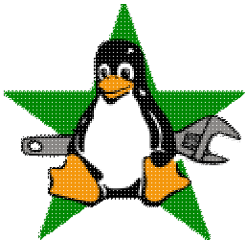
Provide a range of IT services that are non commercial, privacy respecting.

Ethical ISPs providing trusted email and website hosting services to their users have distinguished themselves in the past by protecting users' privacy from government spying and corporate data thiefs.

Opposed to EU data retention bill

aktivix.org antifa.net autistici.org boum.org cat.org.au ecn.org espora.org enzyme.org.nz guardachuva.org interactivist.net linefeed.org moviments.net mutualaid.org nadir.org nodo50.org poivron.org resist.ca riseup.net sarava.org sindominio.net so36.net squat.net tachanka.org taharar.org taktic.org tao.ca kariva.org

aktivix.org



- started operating from 2003
- offered ISP services
- web hosting
- email lists
- personal email
- wiki
- personal VPN
- contact aktivix-request@lists.aktivix.org

activist-networking

Riseup provide are developing software called crabgrass. They are managing an instance of it at http://we.riseup.net

Crabgrass provides an easy way for activists to start campaigns, manage shared documents, upload files, run online polls. Its specifically designed for activists to use and with features that are relevant.

aktivix.org started a blog hosting system called buddypress at http://agitblogs.net

decentralised social networking

Diaspora

web publishing

Indymedia! Indymedia! Indymedia! Indymedia! Indymedia! Indymedia! Indymedia! Indymedia!

email

- Email protocols are generally insecure (ie can be intercepted and read easily)
- Protocols for sending/reading email can be secured (ie use https /imaps /pop3s / starttls)
- Email generally contains hidden envelope information (headers) that can be used to identify sender's IP address

Corporate free email providers

- generally dont support encryption - gmail finally supports https/imaps/pop3s after the chinese hack
- gmail does not do STARTTLS
- hotmail/live/yahoo do not support https/imaps/pop3s/starttls - it's too expensive
- hotmail/yahoo headers contain sender IP address

RTC email providers

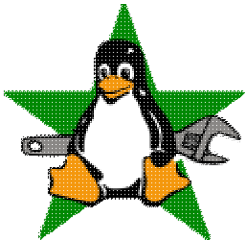
- will only support secure email protocols
- will remove identifying information from headers

gpg

tor

personal vpn

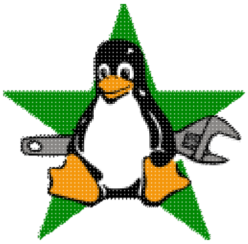
What is 'personal vpn'? A personal VPN encrypts all your internet traffic between your home connection and the provider of the VPN. Then, the traffic goes out onto the regular internet, anonymously bundled in with all the other VPN users. It is faster than tor, and maybe 'good enough' for most things.



A normal VPN is typically about gaining optional access to a trusted network by trusted clients. A personal VPN is the opposite: the clients are not trusted, all their traffic is directed over the VPN out to the public internet, and they cannot connect to other VPN users.

personal vpn - whats it good for

problems that personal vpn can help to fight against:



- data retention of IP address
- some governments that censor the internet. a personal vpn works against chinese government, perhaps not iranian government (you get entirely blocked if they detect all encrypted data stream)
- network and governments that block certain protocols, like skype.
- three strikes laws and other draconian measures to punish people for filesharing.
- ISPs that monitor your DNS usage to make more money off you.
- ISPs that give you only one IP address
- ISPs that use deep packet inspection to practice government surveillance or traffic shaping.
- corporations that track your data and location when you visit their website.
- corporations that only let you use their website if you are from the 'right' country, like hulu.com or spotify.com.