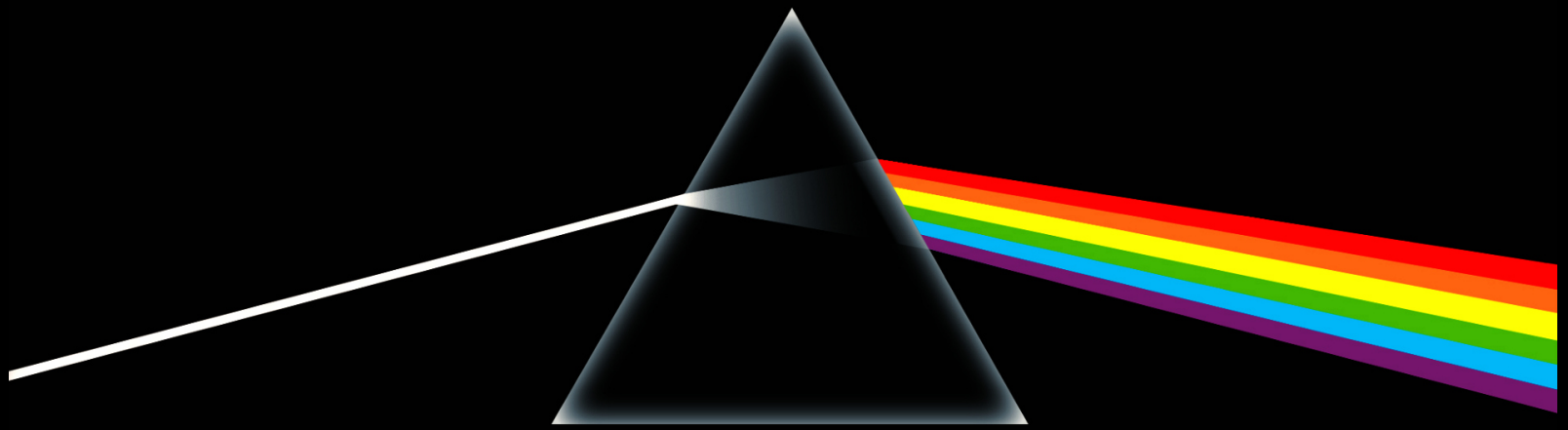


PRISM
&
The Dark Side of the Net

Who am I?

- Mike Harris
- Freelance IT project manager and free software consultant
- Work commercially and for social projects
- Balding
- adelayde@riseup.net
- irc.psand.net #clan

- Network23.org
- TechToolsForActivism.org
- HacktionLab.org
- BristolWireless.net
- BarnCamp.org.uk

Here's the deal

I will...

- Talk about Edward Snowden and PRISM, the impact and what else is going on.
- Discuss whether we think privacy is a right.
- Discuss what we can do about it and look at some tools, with real demos (hopefully).
- Give out some free booklets.
- Go and chill out.

You should...

- Go and chill out.
- Read the booklet.
- Clue-up about this.
- Follow the news and see what issues are cropping up.
- Put some time in to learn some tech and some tools if you want to do something about it.
- Tell your friends about this and about TTFA.

Edward Snowden &

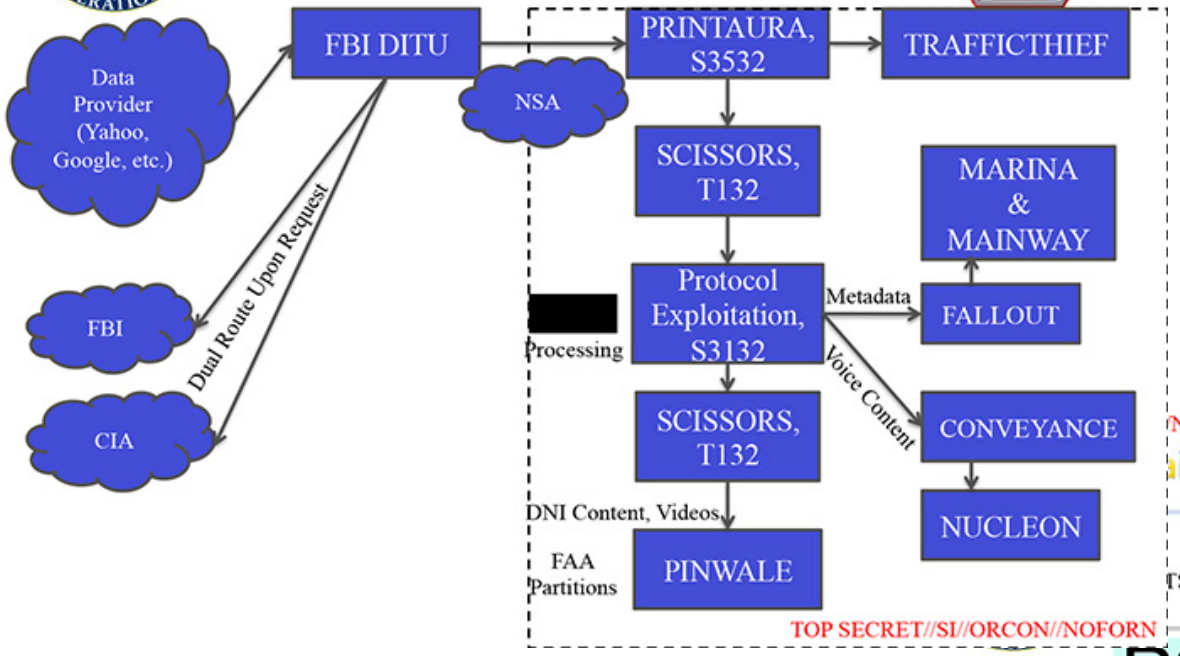
- Snowden was an NSA (National Security Agency) contractor
- Documents were leaked on 6th June 2013 in The Guardian and The Washington Post.
- Explicitly named a number of technology companies in having cooperated with the programme, including: Microsoft, Yahoo!, Google, Facebook, Paltalk, YouTube, AOL, Skype and Apple.
- As a large quantity of Internet traffic is routed via the US, this means that a lot of data is being monitored.
- One claim is that 98% of the production of PRISM data is collected from Yahoo, Microsoft and Google.

What happened next

- Snowden was holed up in Hong Kong then fled to Moscow. He spent weeks at the airport before getting a visa to remain for up to a year. Praise be to Putin the defender of free speech!
- Guardian reporter Alan Rusbridger was contacted by a “very senior UK government official” who demanded the return and destruction of all material that was being worked on at The Guardian threatening legal intervention to shut the newspaper down.

- GCHQ “security experts” oversaw destruction of hard drives on the premises of The Guardian.
- David Miranda, the journalist that broke most of the Snowden stories and Brazilian national, was detained on 19th Aug at Heathrow by UK authorities under section 7 of the Terrorism Act 2000. Under the Act he was not permitted a lawyer. They retained his laptop, phone and various other belongings. http://ttfa.net/miranda (The Guardian)
- Finally, a possibly randomly Anonymous hacked into Mole Valley Council's web site to protest about the detention of Miranda.

(TS//SI//NF) PRISM Collection Dataflow



PRISM

US-984XN

NOFORN

TS//SI//NF) PRISM Case Notations

P2ESQC120001234

PRISM Provider P1: Microsoft P2: Yahoo P3: Google P4: Facebook P5: PalTalk P6: YouTube P7: Skype P8: AOL PA: Apple	
Fixed trigraph, denotes PRISM source collection	
Year CASN established for selector	
Serial #	
Content Type A: Stored Comms (Search) B: IM (chat) C: RTN-EDC (real-time notification of an e-mail event such as a login or sent message) D: RTN-IM (real-time notification of a chat login or logout event) E: E-Mail F: VoIP G: Full (WebForum) H: OSN Messaging (photos, wallposts, activity, etc.) I: OSN Basic Subscriber Info J: Videos . (dot): Indicates multiple types	

PRISM: The ramifications?

- Although this is US legislation, PRISM actually has most effect on the privacy of non-US nationals; in fact it explicitly excludes US nationals.
- We always knew that Big Brother was watching, what we didn't know was the perfidiousness of the cooperation of commercial companies that hold our data and that they are protected under the law.
- We know that the government IS interested in and WILL go to these lengths to MONITOR what we are doing. We know that, whether under pressure or not, companies WILL collude with this as they are legally protected.
- We know that foreign governments will break their own constitutional privacy laws and also those laws of other countries.
- We know that other governments have similar programmes, and that programmes can exchange information … for example:

What else is going on?

- PRISM isn't the only such system: Tempora is run by GCHQ who, according to Snowden, share data that they collect with the NSA. 300 GCHQ and 250 NSA staff are employed to process the data and some 850,000 people have access to it.
- Data carriers are compelled by law to comply with a request for data to be fed in to and processed by Tempora.
- We also have ECHELON (Five Eyes), Schengen Information System, INDECT, Data Retention Directive in the EU, Golden Shield Project (aka Great Firewall of China), Frenchelon in France, NATGRID, Centralised Monitoring System and DRDO NETRA in India, SORM in Russia, Titan in Sweden, Onyx in Switzerland, National DNA Databasein the (UK, Fairview, DCSNet, Main Core, and many others in the US.
- And all the time new legislation, such as the Telecommunications (Interception Capability and Security) Bill in New Zealand are threatening our freedom and privacy further.

Data Retention (DR)

- EU Data Retention Directive* adopted in 2006 – legal requirement for member governments to ensure communications providers retain data for 6 – 24 months.
- Data is required to be available to competent national authorities in specific cases for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.
- In the UK under RIPA (Regulation of Investigatory Powers Act 2000) certain bodies have access to retained data and the Home Office has the power to change this list at any time.
- UK is planning a national centre in Hendon for processing the data collected from the national numberplate recognition system.

* "Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC"

Privacy, a right?

- I believe that we have a right to privacy.
- I believe that it is imperative that we are able to keep our affairs private from the State.
- I believe that the State has no right to our data.
- I believe that Governments should be afraid of their people, not the other way around.
- I believe that privacy is essential to democracy.

Privacy under threat

- Terrorism and child porn, although rare are stirred up as issues by governments and the media and are used to justify legislation that threatens our right to privacy.
- Is the world thus a safer place? Yes child porn is a nasty business, but do we therefore give up all right to privacy? It may be for a benevolent reason so far as we are concerned at this moment, but government's and politics can change like the tides, and will it be dangerous to be right when your government is wrong in the future?
- Let's say the facists get control of the UK or EU in the next 10-15 years: what do we do if they have access to all our communications and maps of everyone we know and everyone those we know know?

What can we do?

- Well, to stop using technology to communicate would be a good starting point.

  > mobile phones, any kind of phone, fax, etc.
  > all internet services
  > electronic payment cards & cheques
  > use of anything that needs a licence (e.g. cars, tv)

But is that realistic?

But I want to keep using my tech What can I do?

- Stop using corporate services that require you to have an account right now. These include Facebook, Twitter, Google+, LinkedIn, Wordpress, YouTube, Skype... try alternatives, such as status.net, network23,
- Minimise your use of any corporate services as much as possible, this includes using Google for searches: try https://duckduckgo.com/ or https://startpage.com/ or other from magazine I read?
- Use free software alternatives for your apps such as Firefox, Thunderbird, LibreOffice, GIMP, Scribus, etc.
- Check out prism-break.org and ttfa.net
- http://www.openstreetmap.org/
- Privacy aware providers http://www.autistici.org/en/index.html riseup.net and aktivix.org noblobgs http://www.mailvelope.com/

Privacy vs Anonymity

- Privacy is that you believe that you have the right to a private life.
- That you believe neither the government, corporations or any third party have a right to contravene your privacy.
- The laws being put in place are taking aware our right to the consensual sharing of our data.
- Often to maintain our privacy we also need to enforce our anonymity.
- Although you can have parts of your life that are public and parts that are private.

- Anonymity is when you don't want people to know who you are, for whatever reason.
- This might include for “honest” political reasons, or for dishonest reasons.
- If you're doing something illegal then you probably don't want to get caught.
- It's less of a right and morally a more difficult question.
- The countermeasures to anonymity also threaten our right to privacy.
- You have to be completely anonymous if you're going to be anonymous.

We'll look at them together but consider them as two separate reasons … let's cross over to the Dark Side....

The Dark (side of the) Net

- The Dark Net has various definitions, but I'm going to say it's any bit of the Internet where the data is not publicaly viewable, accessible or searchable.
- Crypto-anarchists like it.
- So do criminals and other ne’er-do-wells.
- Let's look at ways we can be darker and protect our privacy.

Ways of communicating (more) securely

- HTTPS
- Anonymous browsing: TOR, I2P, Orbot
- Encrypted email
- Anonymised email: Susimail, Cables...
- Trusted providers
- Zero-trail distros: Tails, Privatix, Liberté, IprediaOS
- Encrypted VoIP??

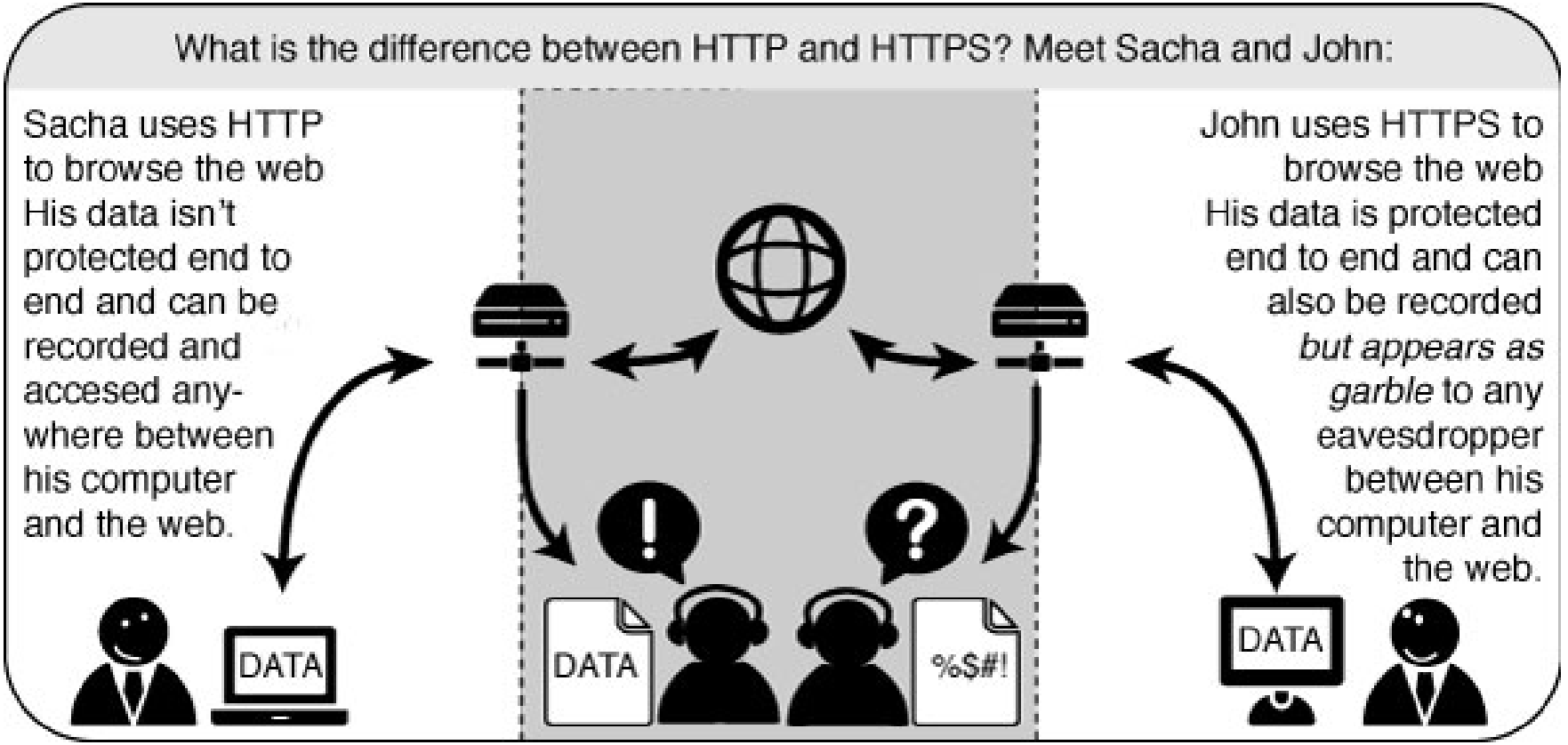
Privacy-aware providers and services

- Aktivix
- Riseup
- Network23
- Austistici
- Noblogs
- Sindominio

- No “IP address” logging.
- Do not keep records of account holders, but will need an email contact.
- Will attempt to fight requests to hand over any data.
- Will have a form of social contract they will require you to comply with.

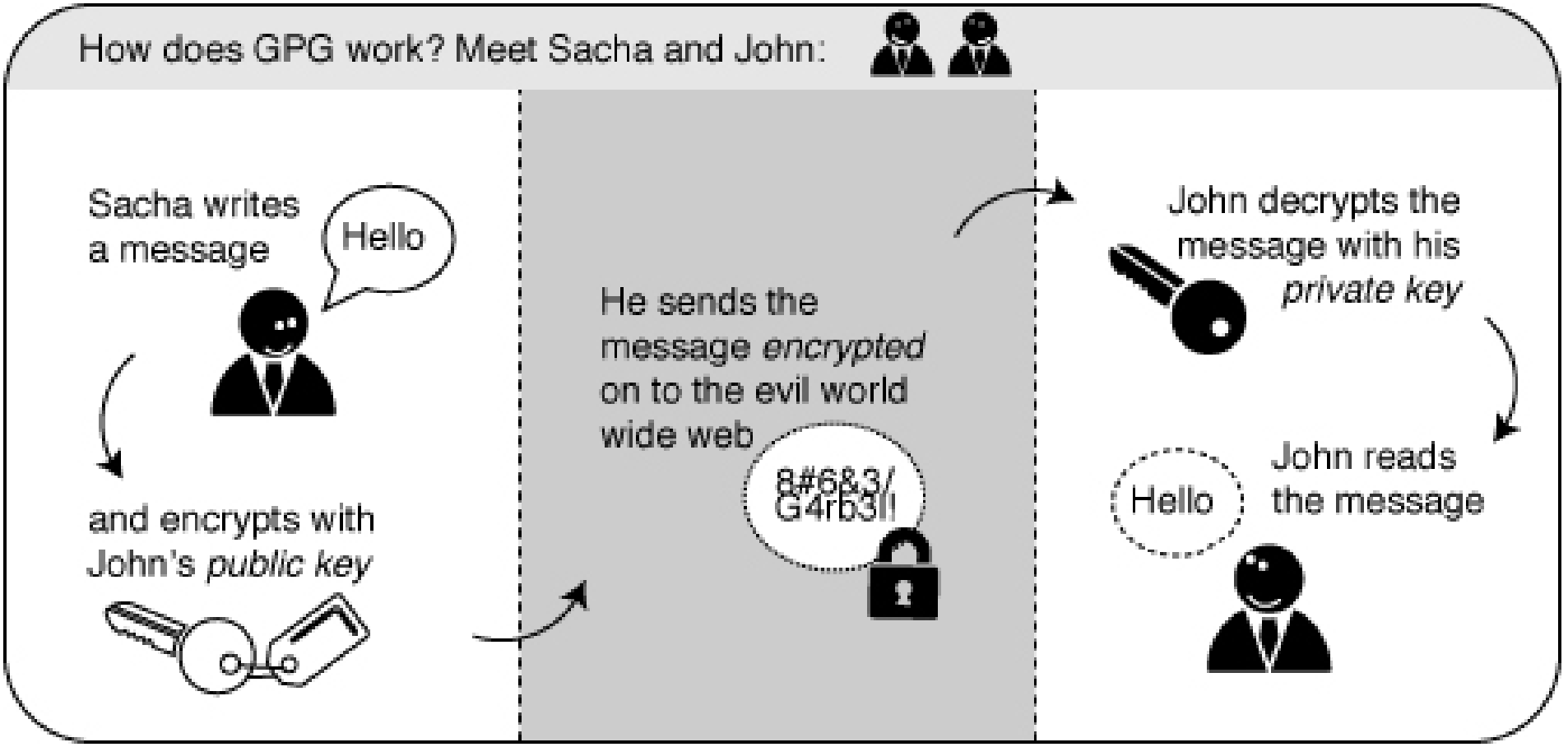
Let's look at https://network23.org briefly...

HTTPS
(= encrypted web browsing)



But is it really safe??

GNU Privacy Guard (GPG) (= encrypted email messages + sender verification)



Email Encryption: GPG

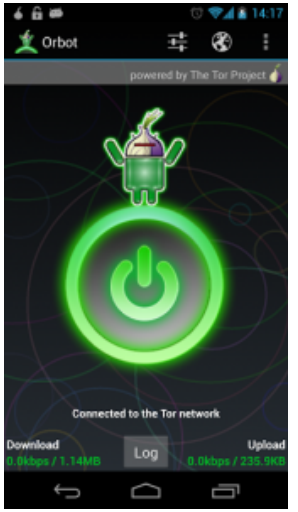
- Options: well it's actually not that trivial to set up sadly, but the benefits are large.
- In my opinion, best option is Thunderbird + Enigmail add-on.
- Mailvelope and ChromeGP plugins for Chrome are good alternatives.
- GPG support is also available via Aktivix's and Riseup's web mail services, and many other providers – check with them.
- You can also use GPG on your local machine and send the encrypted message as an attachment via Gmail, Yahoo, etc.

Secure Communications

- Status.net and identi.ca and indy.im
- Pidgin + OTR
- Xchat + OTR
- Diaspora
- Cryptocat

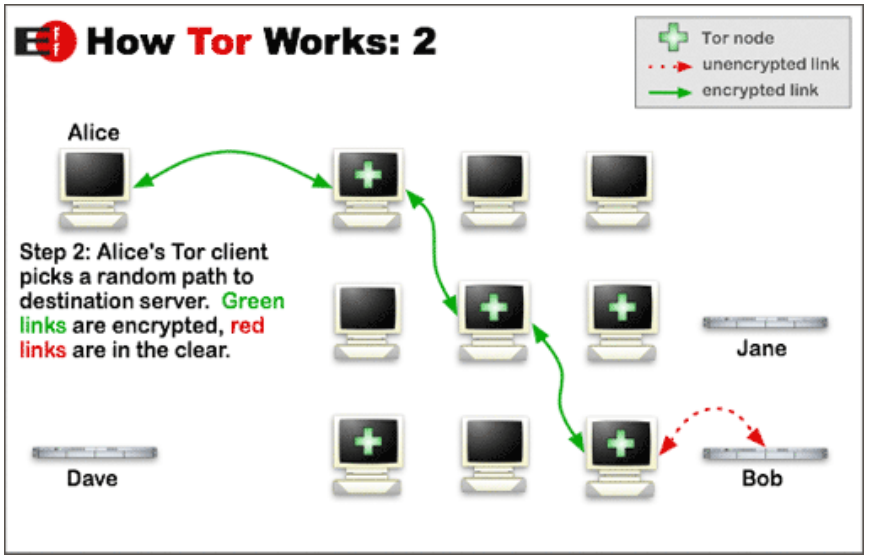
Anonymous Browsing

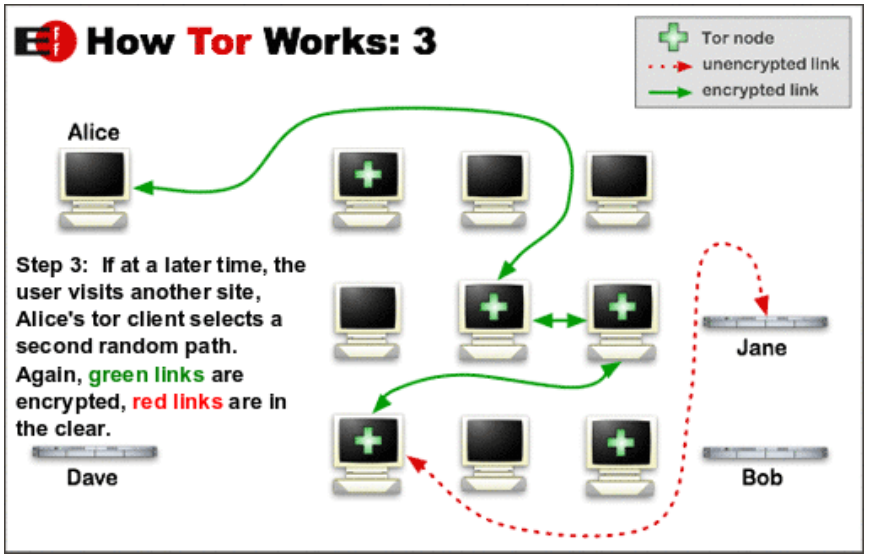
- Firefox + various plug-ins
- TorBrowser
- JonDoBrowser
- Chrome + various plug-ins
- I2P network



TOR

- **T**he **O**nion **R**outer project.
- Tor is a “network of virtual tunnel that allows people to improve their privacy and security on the Internet”.
- https://www.torproject.org
- TOR Browser (Win/Mac/Linux)
- Orbot (Android)
- Recent issue: http://ttfa.net/torbreach





Anonymised Linux Distros

- Specialised Linux distributions. Some examples are: Tails, Privatix, Liberté Linux, IprediaOS & Whonix.
- Use in any computer that can boot up from a CD or USB stick, or from a virtual machine.
- Easy to carry with you.
- Comes configured with everything you need.
- Your “trail” is deleted behind you as soon as you turn off the computer.
- Let´s see one example, TAILS, in action (TAILS = The Amnesic Incognito Live System)

Summary

- Decide what it is that concerns you, what it is you're doing.
- Aim for personal privacy as your base line.
- Minimise your use of corporate solutions, try not to give your data away.
- Support Free Software and Privacy Aware services wherever possible.
- If you need to be anonymous, get with the tools available. Be cautious: is your identify really a secret; can you really trust everyone in your network or cell?
- Read the booklet, check the web, spend some time clueing up, spread the word, be aware, and perhaps, come to BarnCamp 2014!

Thank you

adelayde@riseup.net
99E9 A797 AA7A AE4D 62F5 9364 3F09 AC74
AFD5 5CBF

https://techtoolsforactivism.org
https://hacktionlab.org
https://network23.org
http://prism-break.org