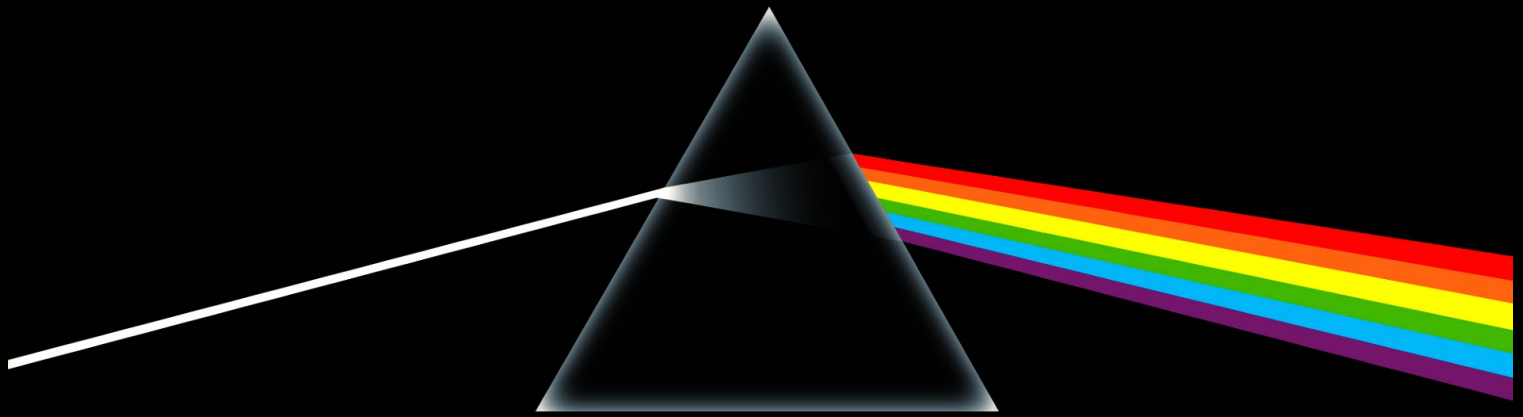


Prism, the Dark Side of the Net, Cyberwar, Cybercrime, Panopticons, Slacktivism and Kittens

The Plan

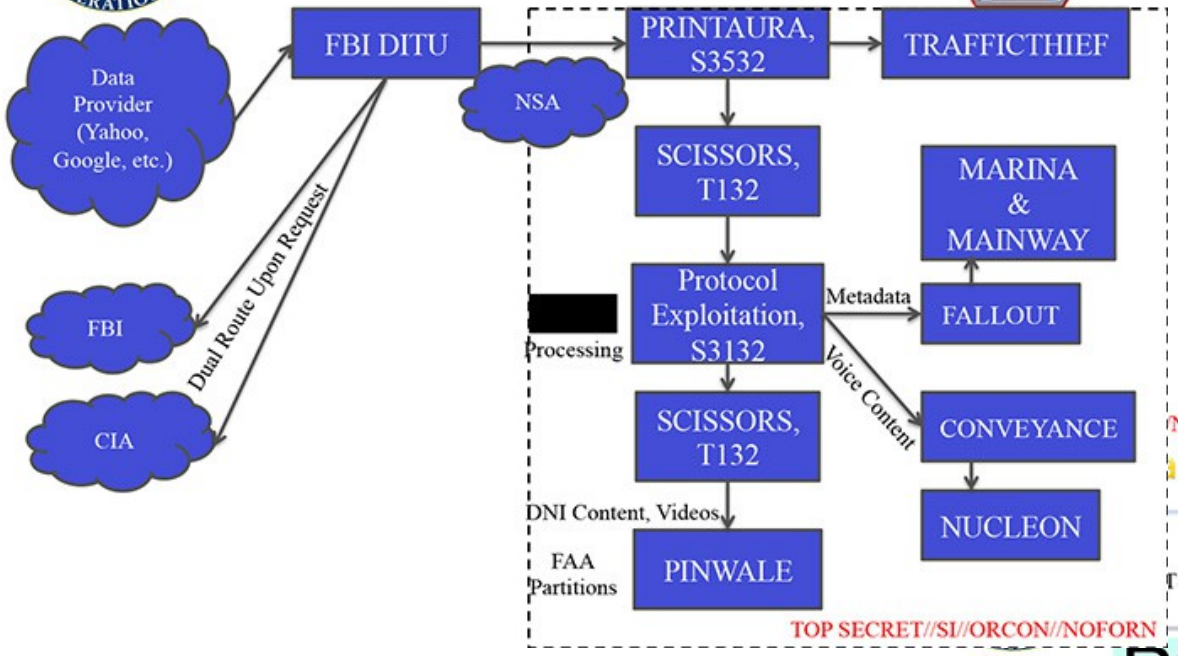
- Talk about Edward Snowden and PRISM
- Discuss what we understand by privacy, what our concerns are and what tools are available.
- Look at activist providers verse commercial providers and why we need the former
- Look at the global internet situation in terms of all the players.
- Fail to come to a conclusion!

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.

TOP SECRET//SI//ORCON//NOFORN

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



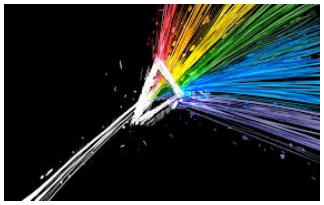
US-984XN

(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	

TOP SECRET//SI//ORCON//NOFORN



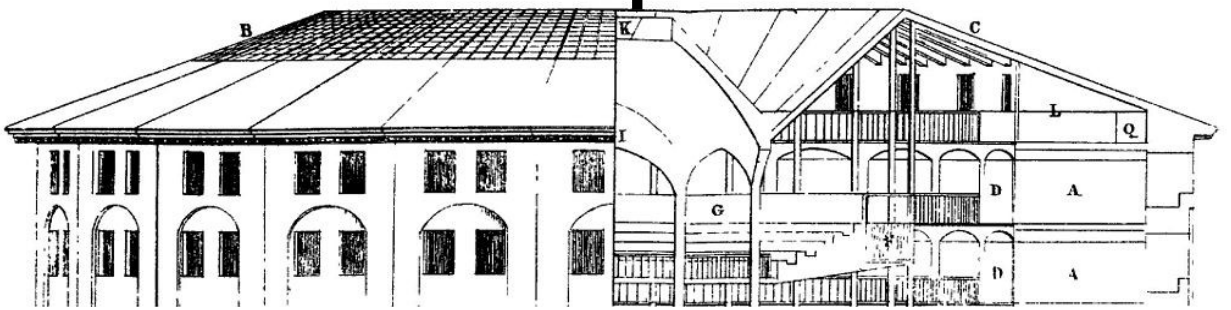
PRISM: The ramifications?

- 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:

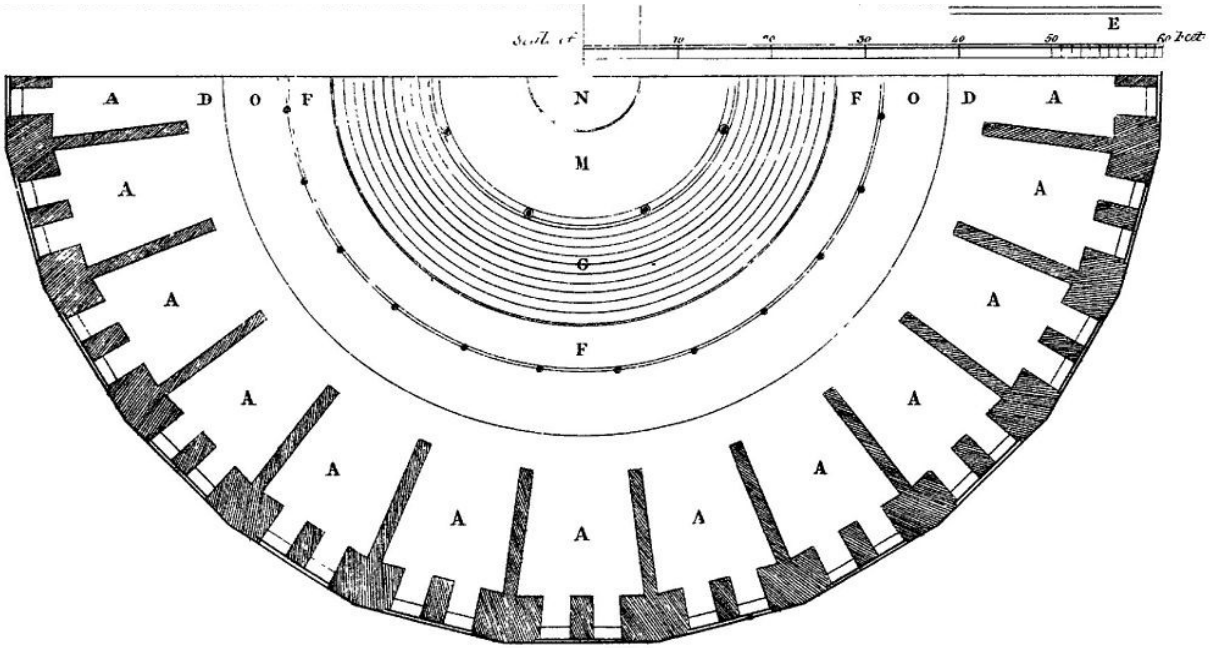
What else is going on?

- 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, RICA in SA, Titan in Sweden, Onyx in Switzerland, National DNA Database in 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.

Panopticon



The mere thought of Prism's existence leads to the idea that we're being monitored all the time and this idea is enough to change our behaviour

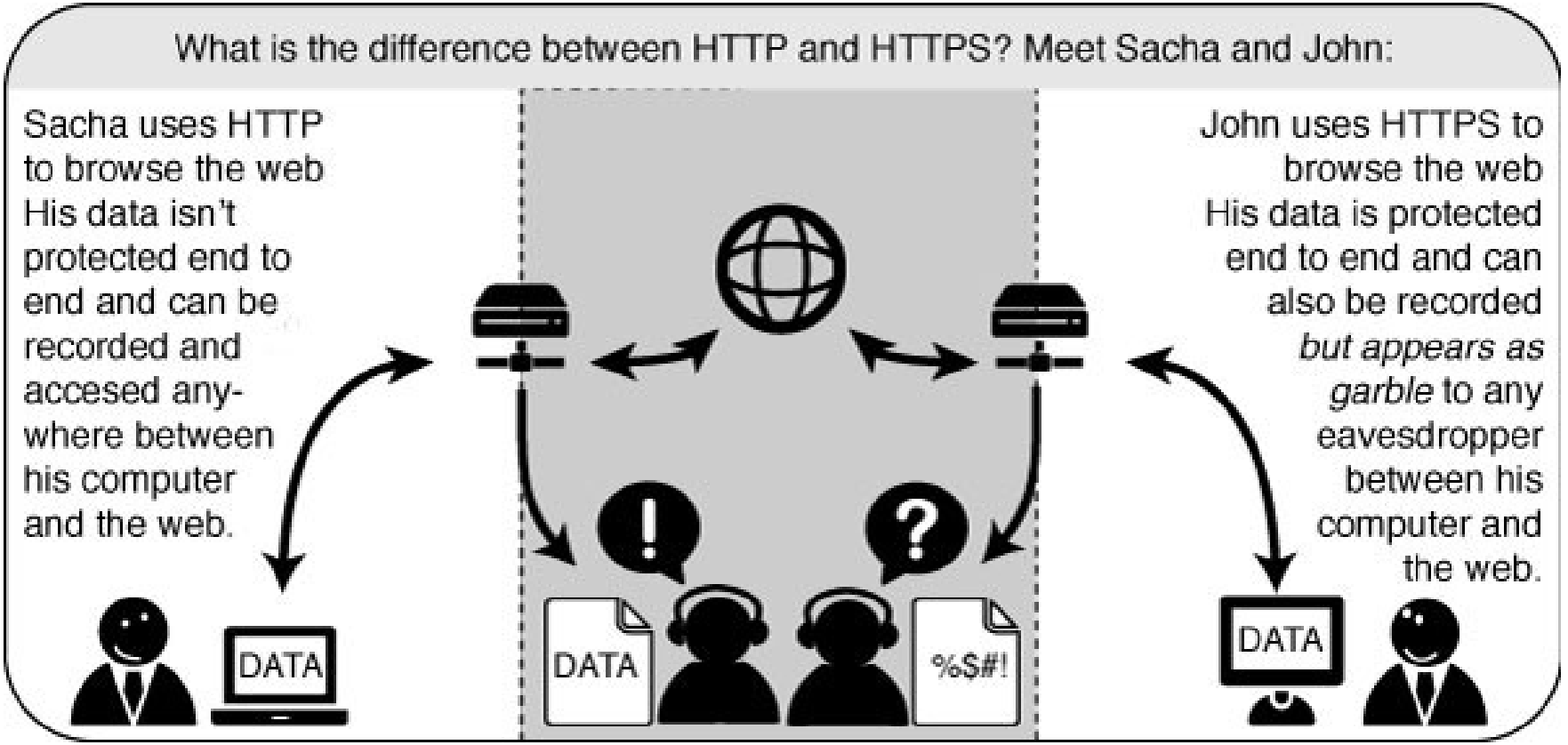


So what can we do?

- Use secure encrypted connections to web sites (HTTPS).
- Use secure encrypted connexions across the Internet (VPNs, TOR and Ssh)
- Use secure encrypted email (GPG)
- Use activist hosting services run by people who respect and uphold your privacy.
- Be more aware of how we communicate and what for

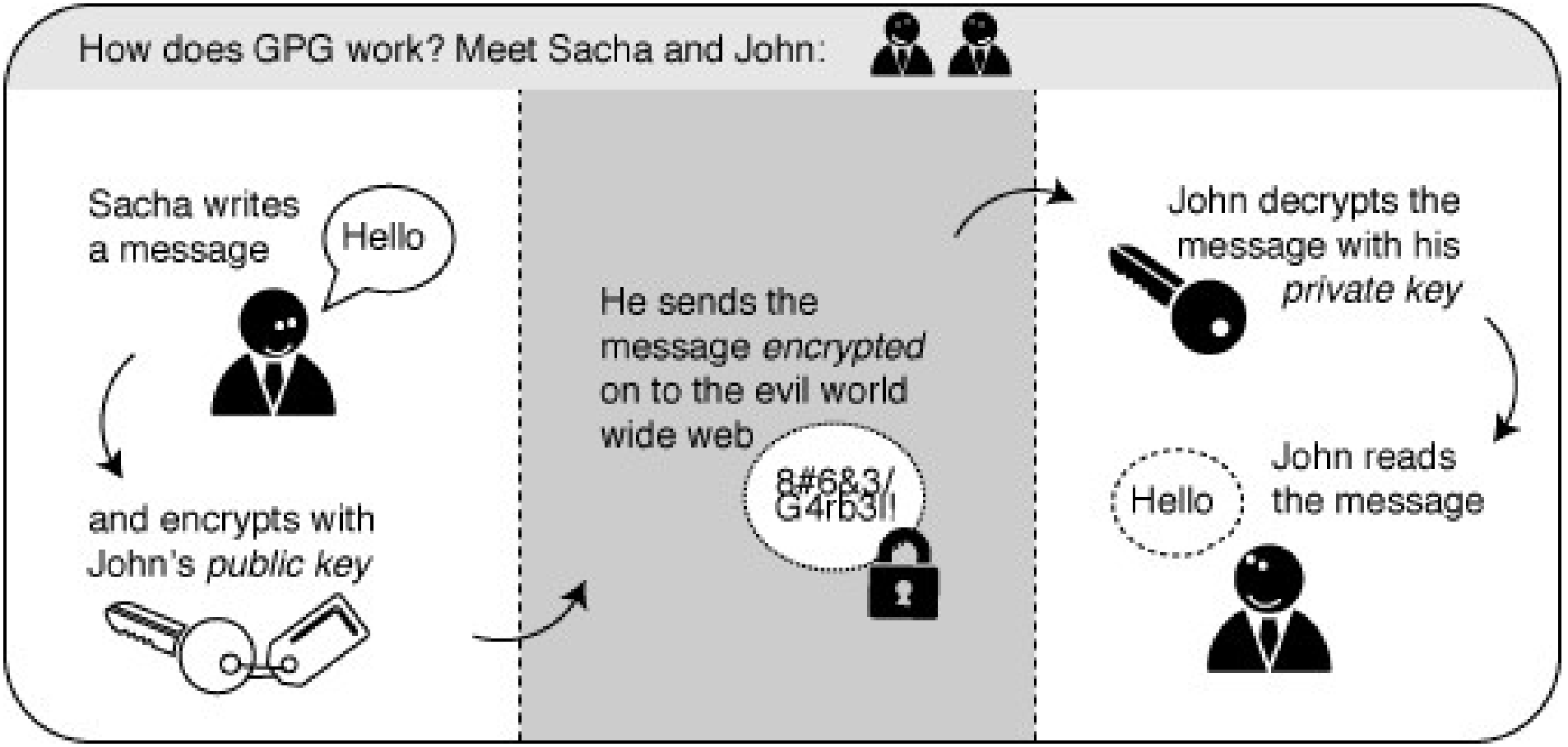
Let's look at some of these….

HTTPS
(= encrypted web browsing)



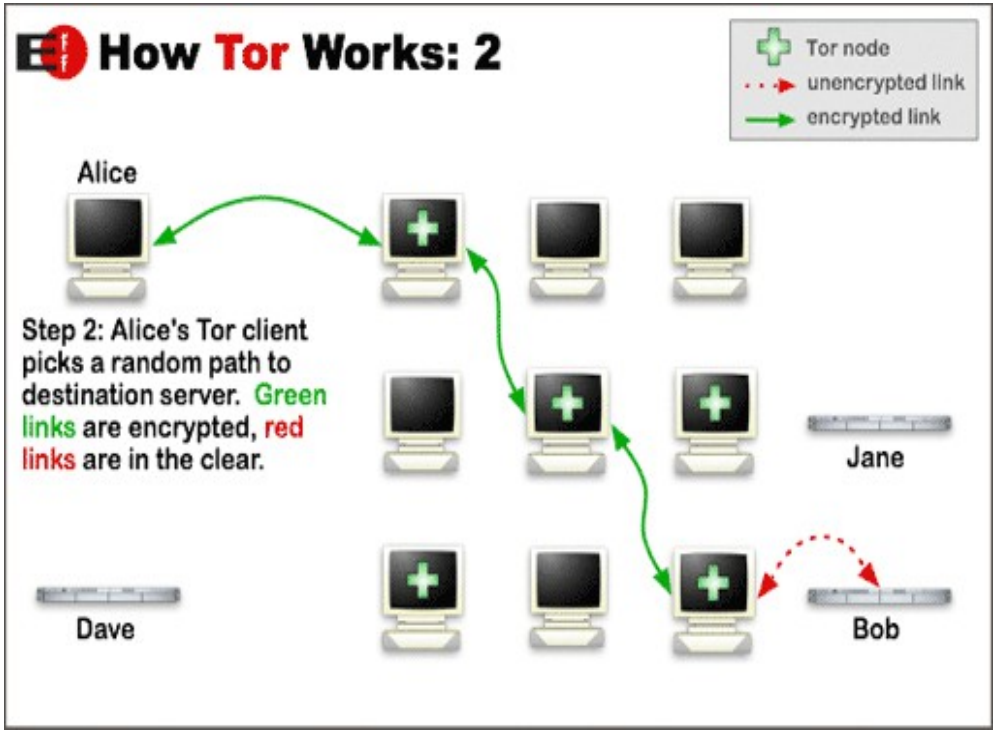
But is it really safe??

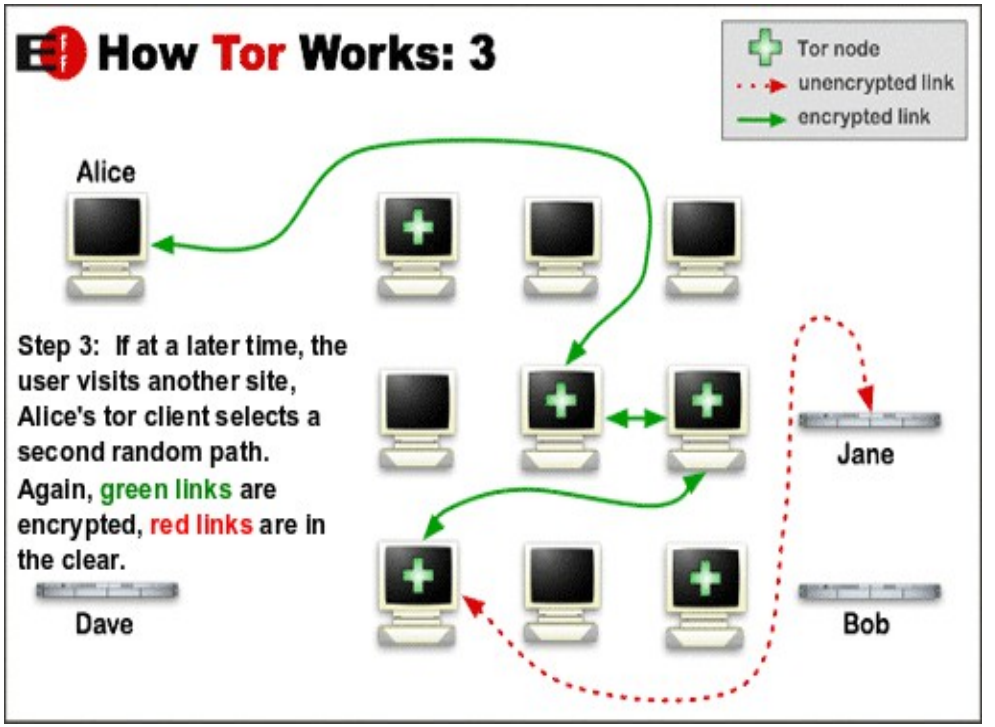
GNU Privacy Guard (GPG) (= encrypted email messages + sender verification)



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





Issues with TOR

- It can be poisened
- It's possible to intercept traffic
- There's a wealth of people using it for unsavoury purposes that make it easy for the media to justify it's evilness.

TAILS = The Amnesic Incognito Live System

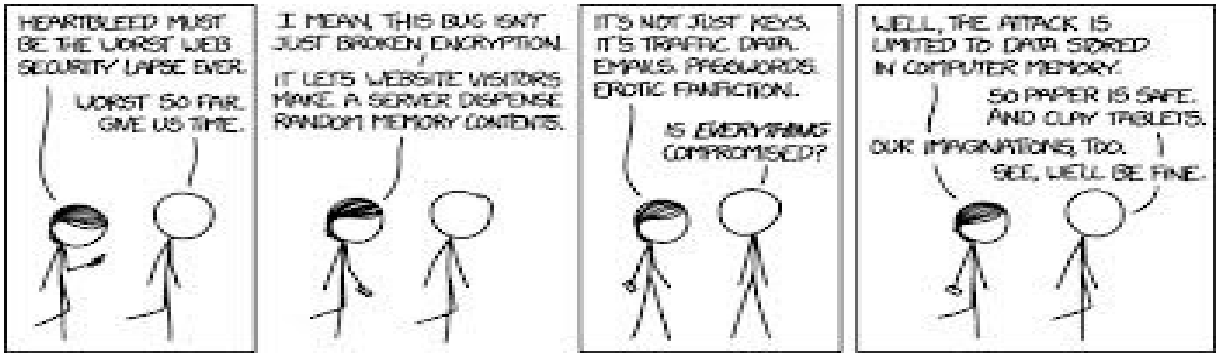
https://tails.boum.org/

HEART BLEED

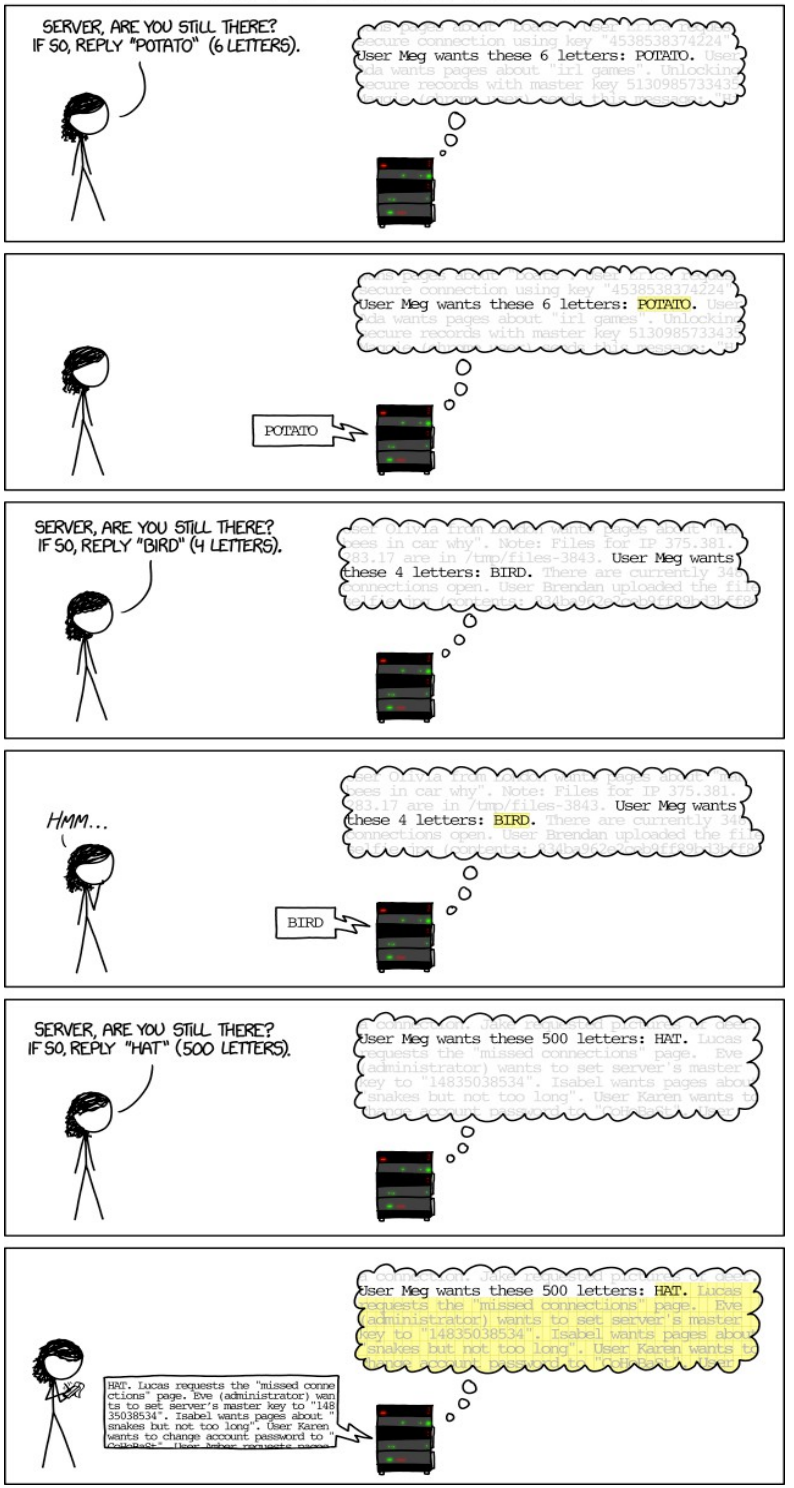
Why buy an SSL toolkit as a black-box when you can get an open one for free?

- Yahoo!
- Aktivix
- Network23
- Pinterest
- Reddit
- Wikipedia
- Mumsnet
- DuckDuckGo
- Riseup
- EventBrite

http://ttfa.net/bleedlist



HOW THE HEARTBLEED BUG WORKS:



http://xkcd.com/1354/

Commercial vs Activist hosting

- Lots of resources for scalability and high traffic
- Continuous expansion and 'improvement' of services
- Large number of staff to support & maintain
- Well-known web addresses for those not-so-activist types
- Support available with SLAs, probably at a cost
- Will log everything you do and will cooperate with authorities
- Will take your site down at any sign of a complaint
- Censorship higher profile and could help breed contempt in citizenry.

- Fewer resources with more difficulty in handling heavy loads
- Can be slow to upgrade resources due to financial limitations
- Often limited and mostly un-paid personnel
- Lesser know web addresses that can be a bit too political for some
- Support can often be sporadic and done in people's spare time.
- Will not log what you do and will 'resist' co-operation with authorities.
- Will resist taking your site down unless absolutely necessary.
- Censorship lower profile as sites less well-known and mostly used by others of a similar political bent.

Questions for activist and Activist Internet Service Providers (AktISPs)

- What purpose does your site serve?
- Does it really need to be hosted on activist servers?
- Are you at risk?
- What audiences are you trying to reach?
- Are you doing anything illegal, unlawful or slanderous?
- What do you expect AktISPs to do about it?
- Have you protected your identity?
- Are you maintaining your privacy on the rest of the net?
- Can you trust you AkISP?
- Do we have the resources to meet the users' expectations?
- How can we respond in good time to issues (such as security alerts, hacks, take-downs)?
- What do we do about take-downs and warrants?
- How to we vet the users? Can we trust them?
- How do we trust *our* service or hardware providers?
- How do we trust each other?
- What do we choose to host? To what level do we support and defend someone's freedom of speech?

What we should be doing...

- We should support our own infrastrucutre – use it or loose it
- Offer time and money to make sure they run
- As AktISPs we need a financial model that is sustainable – through fund-raisers
-

Commercial interests play into the hands of the state panopticon

- Not operating to protect and defend human rights or freedom of speech.
- Operating to provide a benefit to the share-holders.
- Purely commercial angle means they will capitulate at a sneeze, take down your site or hand-over your data.
- An Internet mired in FB status updates, cute kittens, Minecraft and Rick Astley only serves to make it harder for dissidents to get their message out.
- There's increasingly more haystack for the needles to be found in.

Clicktivism (Slacktivism)

- The illusion of Twitter revolutions – the majority of the tweets during the Iranian uprisings of 2009 came from people outside of Iran with various political motivations that we akin the goals of the US Government. Most of what happened, happened on the streets in the traditional way.
- The majority of the World's population aren't on Twitter and have liked the FB page.
- Tweeting isn't a basis for establishing a fully fledged Western-style democracy.
- The Arab Spring could be largely regarded as a disaster.
- Liking or retweeting things is a very passive form of activism.

The Facebook Dilemma

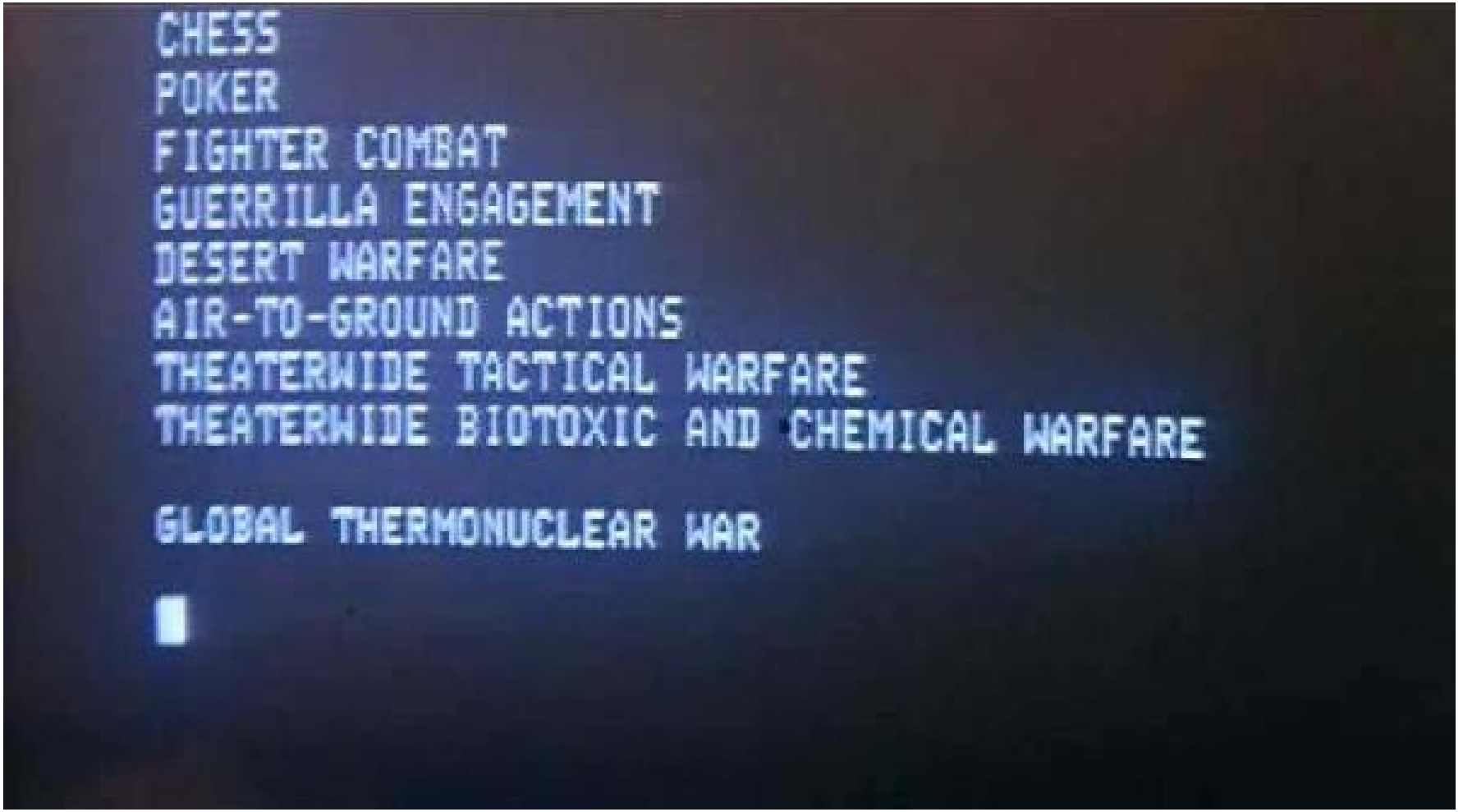
- Has become many people's home page on the Internet, and even many think the internet IS Facebook.
- View of the Internet and World is extremely polarised and filtered due to mechanism of friends and likes.
- Therefore you can easily think that everyone agrees with you and you don't reach out to others.
- Result is a digital “divide and rule” situation.

Double-standards of States

- Want to protect the privacy of the citizens who agree with them.
- Want to further their own political goals and philosophy.
- Want to gain access to information of other states or even disrupt other states.
- Want to the promote the voices of the dissenters of other states

- Want to monitor and limit the opinions of those who disagree with them
- Want to maintain the status quo of the state ideology
- Want to prevent others getting access to their information and their ability to disrupt infrastructure
- Want to minimise the voices of dissenters.

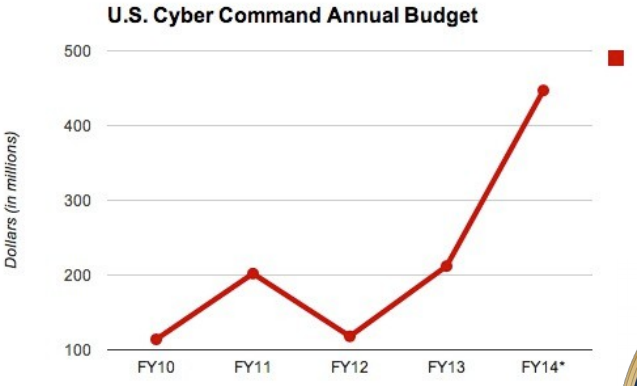
Global Thermonuclear War



Globalised Cyber Warfare

- Theatre of operations: the Internet
- Players: states, military, activists, kitten lovers, drug-dealers, paedophiles, ISIS, hacktivists, banks, patriot hackers, you, me ….
- Weapons: worms, viruses, Stuxnet, etc.
- In 2013 there were over 110,000,000 species of computer viruses collected
- Stuxnet attacked specific hardware – Siemen's WinCC/PCS 7 SCADA control software and only a cascade of centrifuges of a certain size and number (984).
- Chinese military sites we subject to 90,000 attacks from US sources in 2012
- Formed in 2009, USCYBERCOM had a budget of US$1.1 trillion passed in Jan 2014.
- China, Russia and other major protagonists are investing similar resources in a global cyber arms race.
- Nashi in Russia was organised by 120,000 pro-Putin individuals to take on “anti-Fatherland” supporters.
- The Chinese “Black Hawk Safety Net” site has 170,000 members.

Country	Infected computers
Iran	58.85%
Indonesia	18.22%
India	8.31%
Azerbaijan	2.57%
United States	1.56%
Pakistan	1.28%
Others	9.2%



Thank you?

Lean Bytes