

Welcome to

Tor

Paranoia and government hacking

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

`http://www.solidonetworks.com`



<https://www.youtube.com/watch?v=ApRPz9FzkQM>

Source: Lyrics to the old-skool protest song about nuclear war

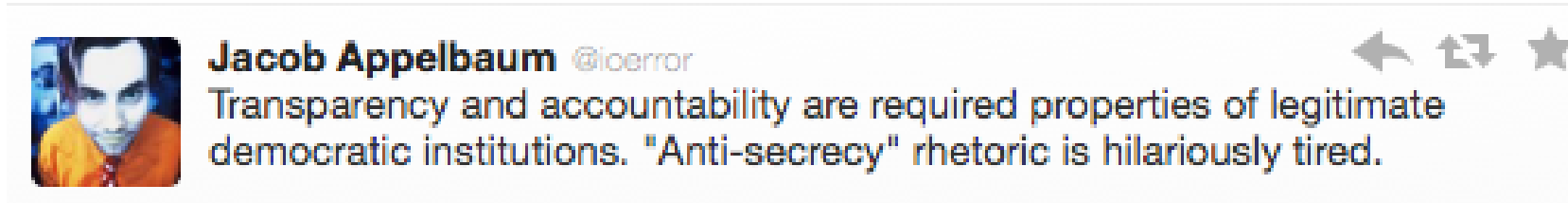
<http://www.fredsakademiet.dk/abase/sange/sang29.htm>

Four days later, his body was found dumped in the Assi River (also spelled: Isa River), with a big, open and bloody wound in his neck where his adam's apple and voice chord had been removed. A clear message to those who dare to raise their voice against the Syrian President Bashar al-Assad.

'Yalla Erhal Ya Bashar' (It's time to leave, Bashar), demanding an end to President Bashar al-Assads regime.

<https://www.youtube.com/watch?v=nox6sVyhBYk>

<http://freemuse.org/archives/5054>



In a democracy we need the citizens with freedom that can act without constant surveillance

Democracy requires that we can actively select which personal data to give up and to whom

Cryptography is peaceful protest against blanket surveillance



Data collected will be **abused** either by criminals or for criminal purposes, commercial purposes no matter what the original intentions were. Today data is gathered to protect us from terrorists, extremism, nazis, pedophiles, abuse of children ... Le mal du jour.

but also enables stalking, employers doing abusive monitoring, spouses and parents abusing power, politicians abusing power, police investigations into legal protests

You should take control of your data - that is democracy


Why think of security?



Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world. A Cypherpunk's Manifesto by Eric Hughes, 1993

Copied from <https://cryptoparty.org/wiki/CryptoParty>

par·a·noi·a

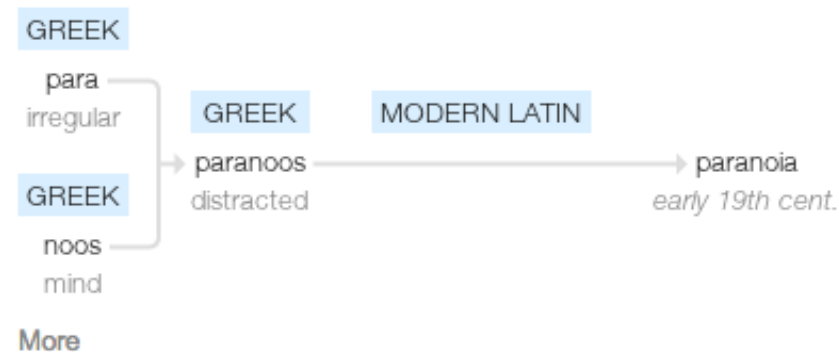
/ˌparəˈnoiə/ 

noun

noun: **paranoia**

1. a mental condition characterized by delusions of persecution, unwarranted jealousy, or exaggerated self-importance, typically elaborated into an organized system. It may be an aspect of chronic personality disorder, of drug abuse, or of a serious condition such as schizophrenia in which the person loses touch with reality.
synonyms: [persecution complex](#), [delusions](#), [obsession](#), [psychosis](#) [More](#)
- suspicion and mistrust of people or their actions without evidence or justification.
"the global paranoia about hackers and viruses"

Origin



Source: google paranoia definition - Er du passende paranoid?

From the definition:

suspicion and mistrust of people or their actions **without evidence or justification. "the global paranoia about hackers and viruses"**

It is not paranoia when:

- Criminals sell your credit card information and identity theft
- Trade infected computers like a commodity
- Governments write laws that allows them to introduce back-doors - and use these
- Governments do blanket surveillance of their population
- Governments implement censorship, threaten citizens and journalist

You are not paranoid when there are people actively attacking you!

Information Risk Management

Life is full of risk.

Risk is the possibility of damage happening and the ramifications of such damage should it occur. *Information risk management (IRM)* is the *process* of identifying and assessing risk, reducing it to an acceptable level, and implementing the right mechanisms to maintain that level. There is no such thing as a 100 percent secure environment. Every environment has vulnerabilities and threats to a certain degree. The skill is in identifying these threats, assessing the probability of them actually occurring and the damage they could cause, and then taking the right steps to reduce the overall level of risk in the environment to what the organization identifies as acceptable.

Source: Shon Harris *CISSP All-in-One Exam Guide*



Using crypto is a peaceful protest
and it is not magic



What if I told you:

Governments will introduce back-doors

Intercepting encrypted communications with fake certificates - check

May 5, 2011 A Syrian Man-In-The-Middle Attack against Facebook

"Yesterday we learned of reports that the Syrian Telecom Ministry had launched a man-in-the-middle attack against the HTTPS version of the Facebook site."

Source:

<https://www.eff.org/deeplinks/2011/05/syrian-man-middle-against-facebook>

Mapping out social media and finding connections - check

Infecting activist machines - check

Tibet activists are repeatedly being targeted with virus and malware, such as malicious apps for Android like KakaoTalk

Tor-users infected with malicious code to reveal their real IPs

<https://blog.torproject.org/blog/hidden-services-current-events-and-freedom-hosting>

Copying journalist data in airports - check



NSA - need we say more?

[http://en.wikipedia.org/wiki/PRISM_\(surveillance_program\)](http://en.wikipedia.org/wiki/PRISM_(surveillance_program))

Governments also implementing censorship

Outlaw and/or discredit crypto

Go after Tor exit nodes

The only users of Tor are bad people, BAD people I tell you!

Criminals

Drugs - lots of drugs

Terrorists planning World War IIIII

Pedophiles

More drugs - and high quality!

Copyright infringement



Did you know the roads are being used by criminals in the physical world



<http://www.onion-router.net/>

This website comprises the onion-router.net site formerly hosted at the Center for High Assurance Computer Systems of the U.S. Naval Research Laboratory. It primarily covers the work done at NRL during the first decade of onion routing and reflects the onion-router.net site roughly as it existed circa 2005. As a historical site it may contain dead external links and other signs of age.



- Tor was originally designed, implemented, and deployed as a third-generation onion routing project of the U.S. Naval Research Laboratory.
- Today, it is used every day for a wide variety of purposes by **normal people, the military, journalists, law enforcement officers, activists, and many others.**
- Tor's **hidden services** let users publish web sites and other services

Source:

<https://www.torproject.org/about/overview.html.en>



Dan Egerstad, Swedish computer security consultant obtained log-in and password information for 1,000 e-mail accounts belonging to foreign embassies, corporations and human rights organizations.

Use encryption and secure protocols AND Tor!

Note: I have no knowledge about the danish embassies using or not using Tor, but probably they do.



Danish police and TAX authorities have the legal means, even for small tax-avoidance cases, see *Rockerloven*

Danish prime minister Helle Thorning-Schmidt does NOT criticize the USA

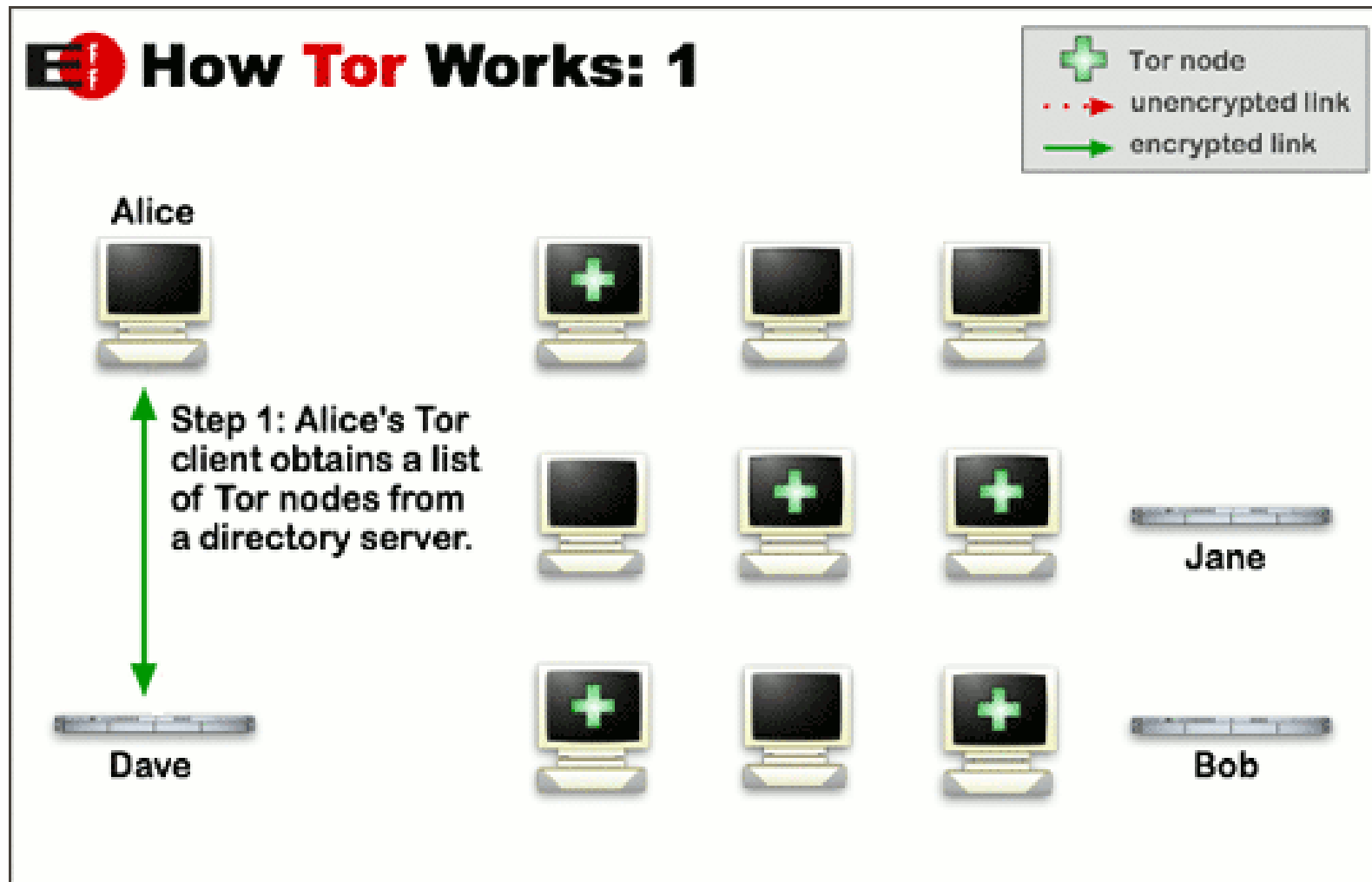


What if I told you:

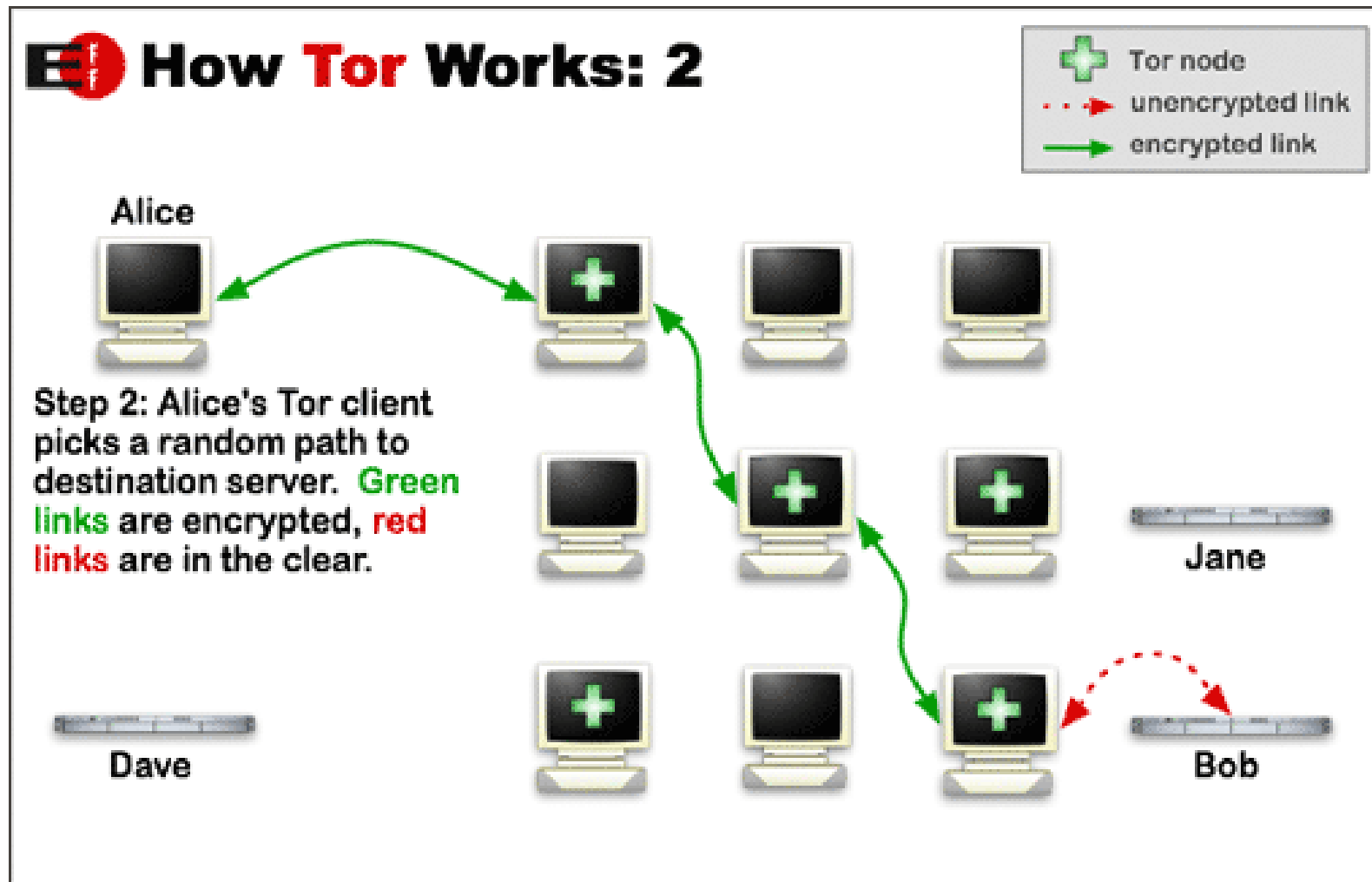
Criminals will be happy to leverage backdoors created by government

It does not matter if the crypto product has a weakness to allow investigations or the software has a backdoor to help law enforcement. Data and vulnerabilities WILL be abused and exploited.

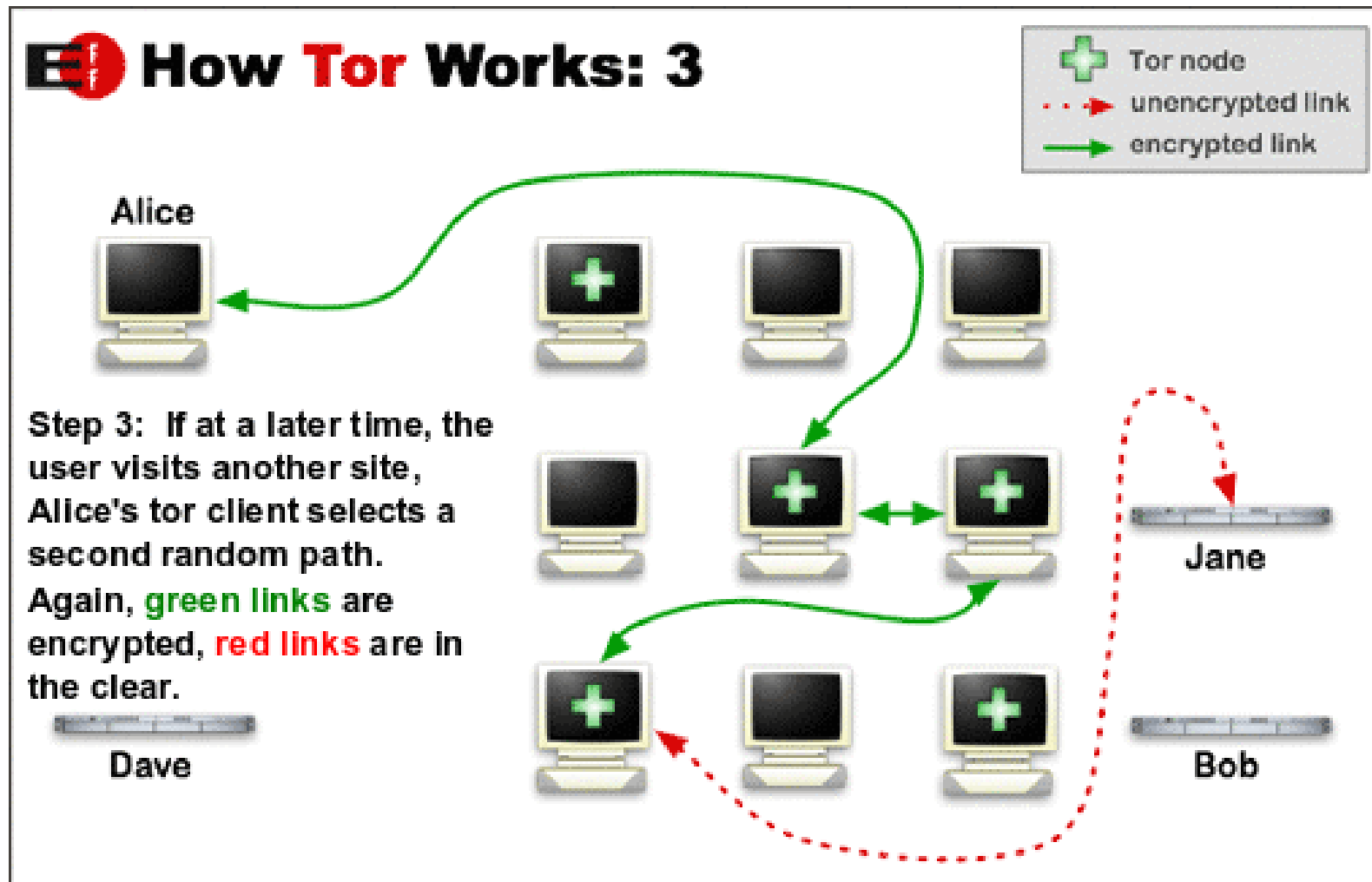
If nothing else Snowden leaks have shown us - trust nobody!



pictures from <https://www.torproject.org/about/overview.html.en>

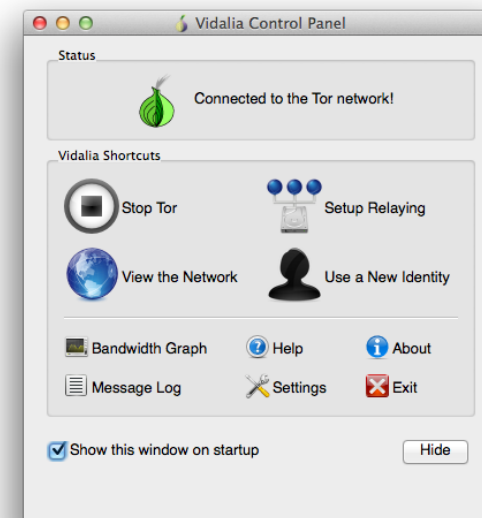
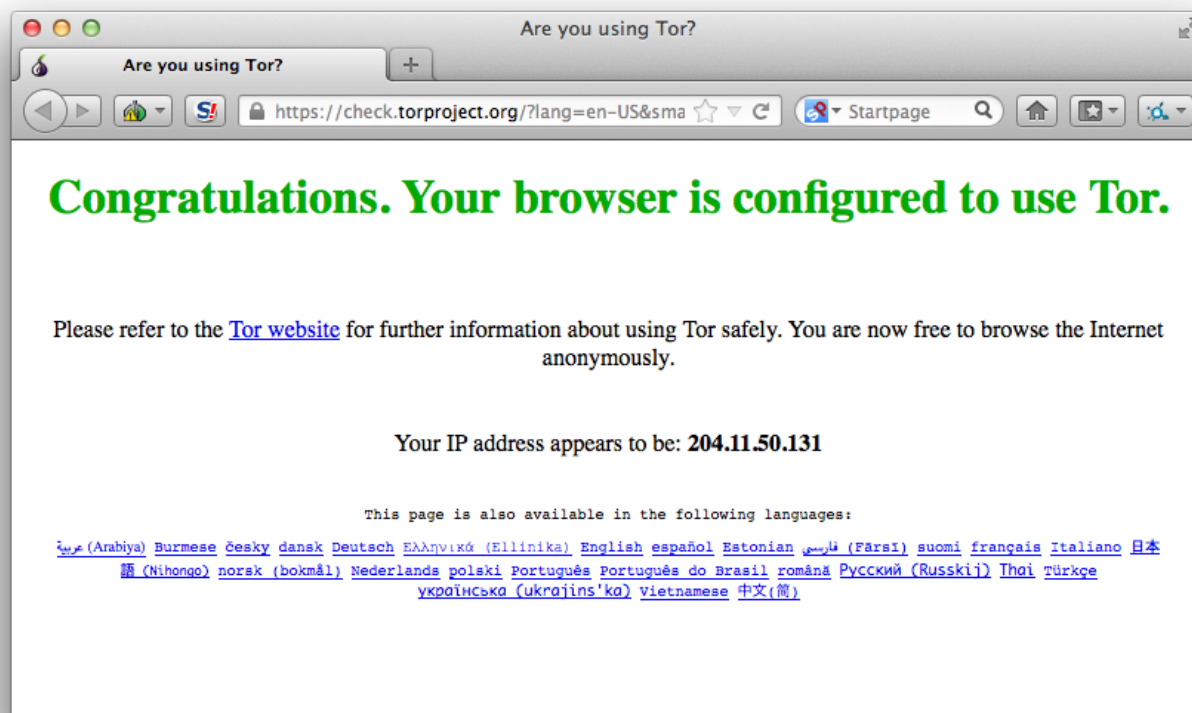


pictures from <https://www.torproject.org/about/overview.html.en>



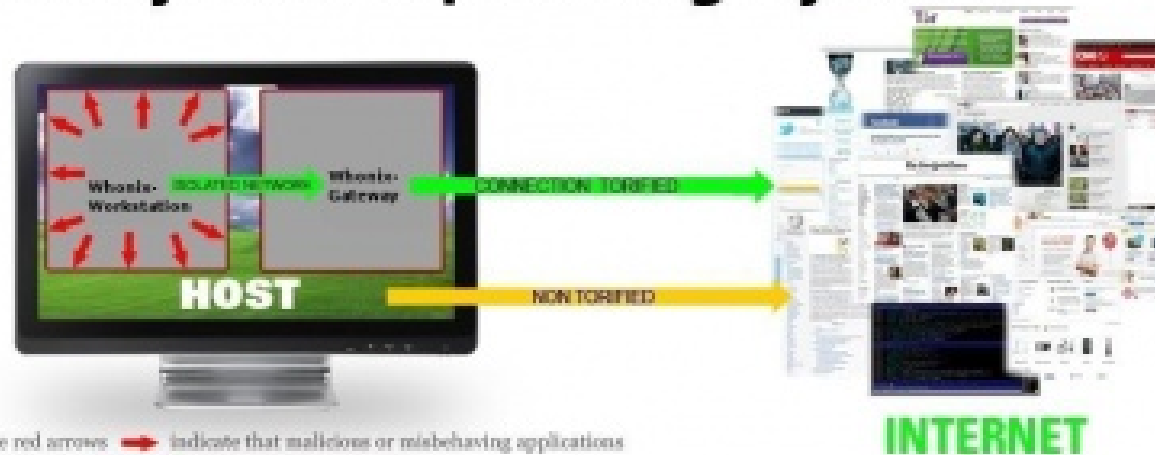
pictures from <https://www.torproject.org/about/overview.html.en>

Recommendation is to run Tor browser



Also plugins to Firefox etc. beware of browser fingerprint and DNS leaks!

Whonix Anonymous Operating System



The red arrows ➡ indicate that malicious or misbehaving applications can't break out of the Whonix-Workstation. All network connections ➡ are forced to go through Whonix-Gateway, where they are torified and routed to the Internet.

Whonix is an operating system focused on anonymity, privacy and security. It's based on the Tor anonymity network[5], Debian GNU/Linux[6] and security by isolation. DNS leaks are impossible, and not even malware with root privileges can find out the user's real IP.

<https://www.whonix.org/>

Tor is still DHE 1024 (NSA crackable)

By Robert Graham

After more revelations, and expert analysis, we still aren't precisely sure what crypto the NSA can break. But everyone seems to agree that if anything, the NSA can break 1024 RSA/DH keys. Assuming no "breakthroughs", the NSA can spend \$1 billion on custom chips that can break such a key in a few hours. We know the NSA builds custom chips, they've got fairly public deals with IBM foundries to build chips.

The problem with Tor is that it still uses these 1024 bit keys for much of its crypto, particularly because most people are still using older versions of the software. The older 2.3 versions of Tor uses keys the NSA can crack, **but few have upgraded to the newer 2.4 version with better keys.**

Source:

<http://blog.erratasec.com/2013/09/tor-is-still-dhe-1024-nsa-crackable.html>

After the last round of revelations from Edward Snowden, described as "explosive" by Bruce Schneier, several threads started on the tor-talk mailing list to discuss Tor cryptography. A lot of what has been written is speculative at this point. But some have raised concerns about 1024 bit Diffie-Hellman key exchange. **This has already been addressed with the introduction of the "ntor" handshake in 0.2.4 and Nick Mathewson encourages everybody to upgrade.**

Source:

<https://blog.torproject.org/blog/tor-weekly-news-%E2%80%94-september-11th-2013>

- **Tor blog** Great news stories about Tor
<https://blog.torproject.org/blog/>
- **Electronic Frontier Foundation (EFF)**
<https://www.eff.org/>
- **Tor users are also Access users**
<https://www.accessnow.org/>
- **cryptoparty.org and Asher Wolf**
<https://en.wikipedia.org/wiki/CryptoParty> https://twitter.com/Asher_Wolf
- **Schneier on Security**
<https://www.schneier.com/>
Sample analysis How the NSA Attacks Tor/Firefox Users With QUANTUM and FOXACID
https://www.schneier.com/blog/archives/2013/10/how_the_nsa_att.html
- **Cryptome welcomes documents for publication that are prohibited by governments worldwide**
cryptome.org/

MOBILIZING FOR GLOBAL DIGITAL FREEDOM JOIN US! Email country [Join!](#)

 **access**

[Home](#) | [Campaigns](#) | [Policy](#) | [Blog](#) | [Calendar](#) | [About](#) | [Donate](#)

 **STOP WATCHING US**



THANK YOU

the rally's over, but we're just getting started.

StopWatchingUs: We're Just Getting Started.

Thank you. You and more than 3,500 other people turned out yesterday to protest the NSA's mass surveillance program. The rally's over now, but we're just getting started.

[Stay Connected »](#)

Access defends and extends the digital rights of users at risk around the world. By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all.

Tor Network Status -- Router Detail

General Information	
Router Name:	kramse
Fingerprint:	3C5D F71E 0358 B535 4FC3 9847 4CED BC27 88DE E62F
Contact:	Henrik Lund Kramshøj <hlk AT solido dot net>
IP Address:	94.126.178.1
Hostname:	tor-exit01.solidonetworks.com
Onion Router Port:	9001
Directory Server Port:	9030
Country Code:	DK
Platform / Version:	Tor 0.2.4.17-rc on FreeBSD
Last Descriptor Published (GMT):	2013-11-04 01:49:54
Current Uptime:	14 Day(s), 10 Hour(s), 56 Minute(s), 3 Second(s)
Bandwidth (Max/Burst/Observed - In Bps):	524288000 / 524288000 / 7262872
Family:	No Info Given

solidaritetskryptering

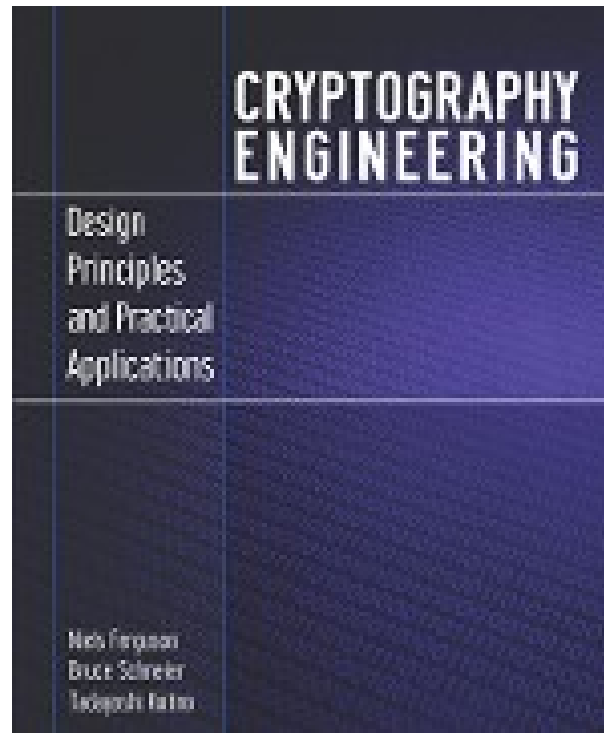
more expensive to do *blanket surveillance* and focus will switch to targeted monitoring!



Hey, Lets be careful out there!

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

Source: Michael Conrad <http://www.hillstreetblues.tv/>



Cryptography Engineering by Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno

<https://www.schneier.com/book-ce.html>



HTTPS Everywhere is a Firefox extension produced as a collaboration between The Tor Project and the Electronic Frontier Foundation. It encrypts your communications with a number of major websites.

`http://www.eff.org/https-everywhere`

And configure your browser to not activate content like Flash before you click

Plugins like NoScript for Firefox and NotScripts for Chrome is highly recommended

Officers use counter-terrorism laws to remove a mobile phone from any passenger they wish coming through UK air, sea and international rail ports and then scour their data.

The blanket power is so broad they do not even have to show reasonable suspicion for seizing the device and can retain the information for "as long as is necessary".

Data can include call history, contact books, photos and who the person is texting or emailing, although not the contents of messages.

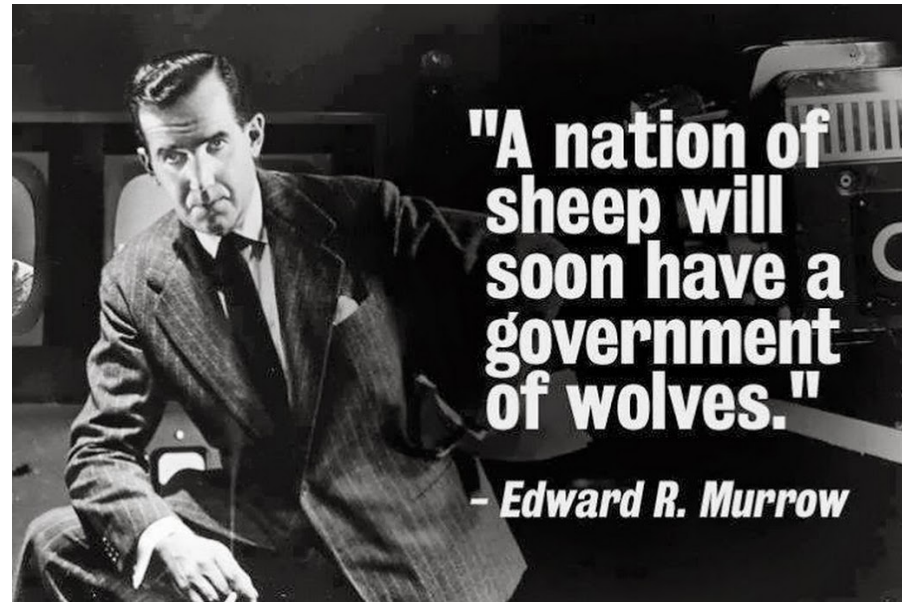
Source: <http://www.telegraph.co.uk/technology/10177765/Travellers-mobile-phone-data-seized-by-police-at-border.html>

(Reuters) - British authorities came under pressure on Monday to explain why anti-terrorism powers were used to detain for nine hours the partner of a journalist who has written articles about **U.S. and British surveillance programs** based on **leaks from Edward Snowden**.

Brazilian David Miranda, the partner of American journalist Glenn Greenwald, was detained on Sunday at London's Heathrow Airport where he was in transit on his way from Berlin to Rio de Janeiro. **He was released without charge.**

Source:

<http://www.reuters.com/article/2013/08/19/us-britain-snowden-detention-idUSBRE97I0J520130819>



Nothing new really, see for example D.I.R.T and Magic Lantern

D.I.R.T - Data Interception by Remote Transmission since the late 1990s

<http://cryptome.org/fbi-dirt.htm>

<http://cryptome.org/dirty-secrets2.htm>

They will always use *Le mal du jour* to increase monitoring

FBI Carnivore

"... that was designed to monitor email and electronic communications. It used a customizable packet sniffer that can monitor all of a target user's Internet traffic." [http://en.wikipedia.org/wiki/Carnivore_\(software\)](http://en.wikipedia.org/wiki/Carnivore_(software))

NarusInsight "Narus provided Egypt Telecom with Deep Packet Inspection equipment, a content-filtering technology that allows network managers to inspect, track and target content from users of the Internet and mobile phones, as it passes through routers on the information superhighway. Other Narus global customers include the national telecommunications authorities in Pakistan and Saudi Arabia, ..."

<http://en.wikipedia.org/wiki/NarusInsight>