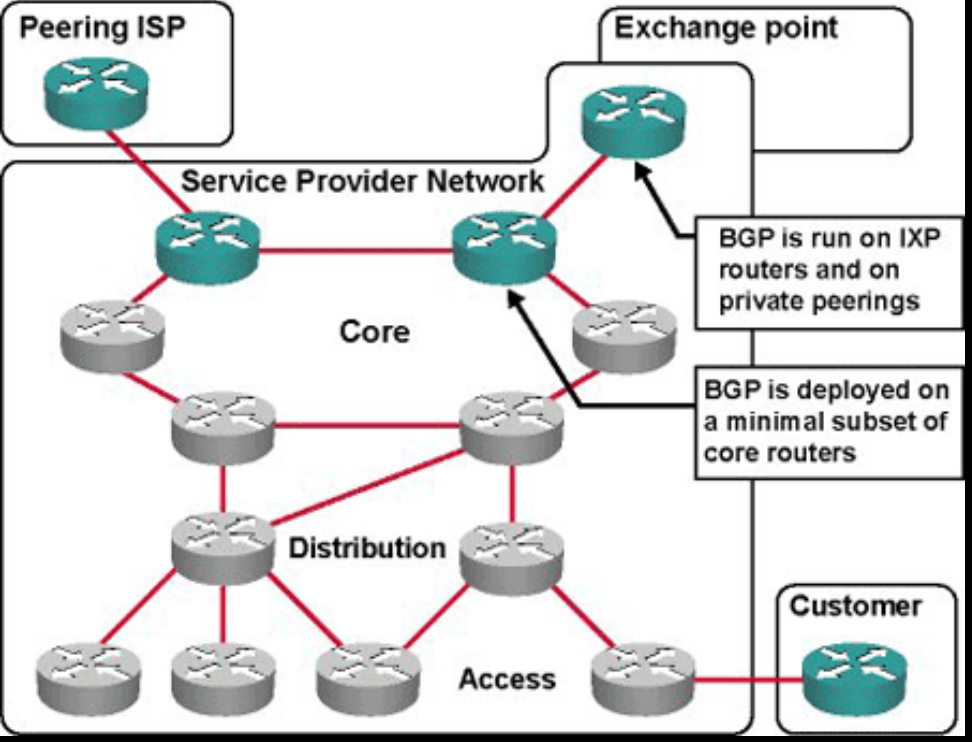
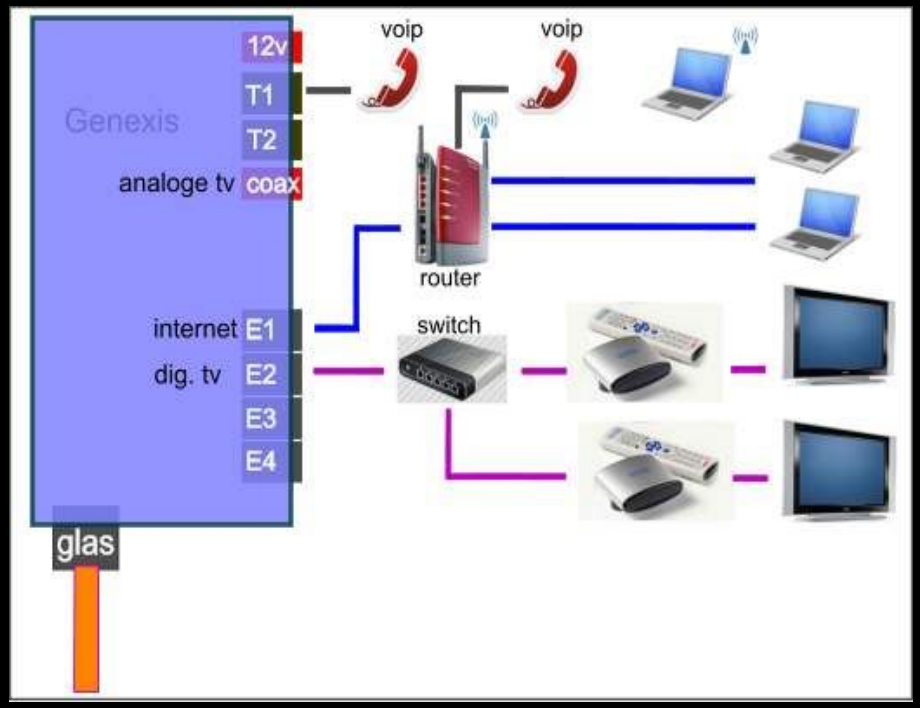
Van Nakamoto tot Snowden
Snowden & Internet

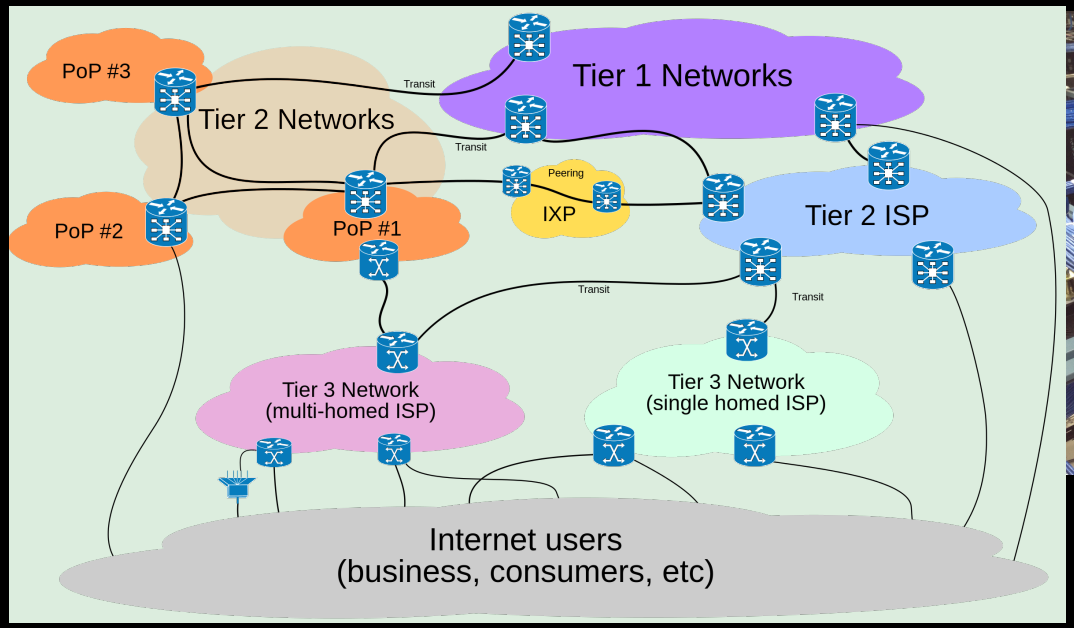
Cees de Laat

Snowden personalia

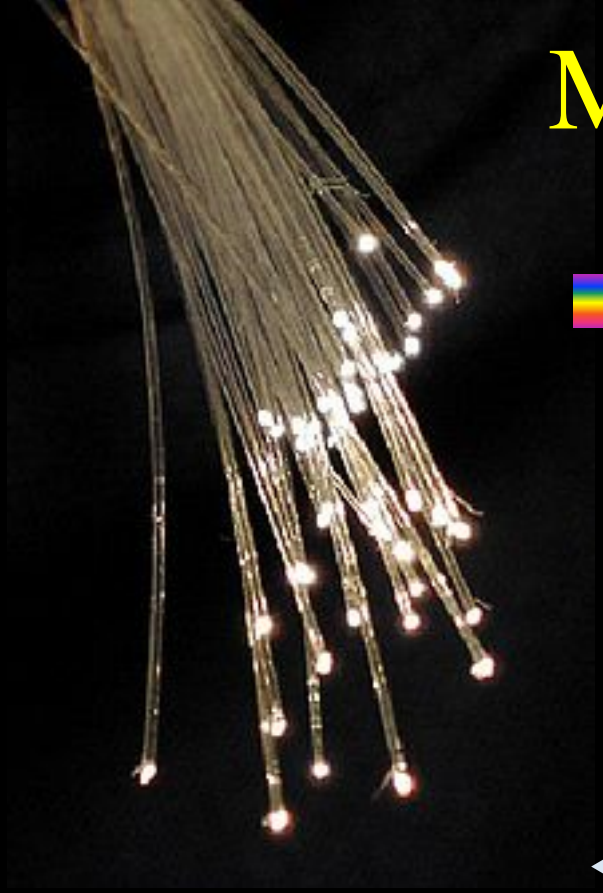
- Edward Joseph Snowden
- Elizabeth City, 21 juni 1983
- voormalig medewerker van de CIA
- Systeembeheerder via het bedrijf Booz Allen Hamilton voor de Amerikaanse veiligheidsdienst NSA werkte
- Snowden lekte in juni 2013 informatie over een reeks van spionageactiviteiten door het NSA op internet

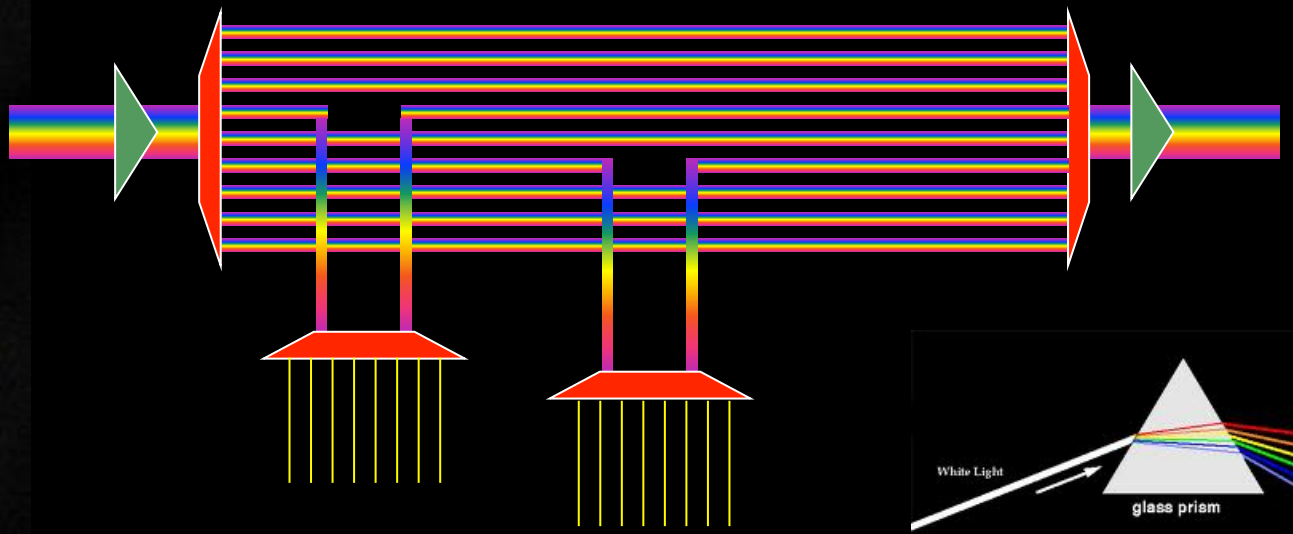

Peering ISP
Exchange point
Service Provider Network
BGP is run on IXP routers and on private peerings
Core
BGP is deployed on a minimal subset of core routers
Distribution
Customer
Access

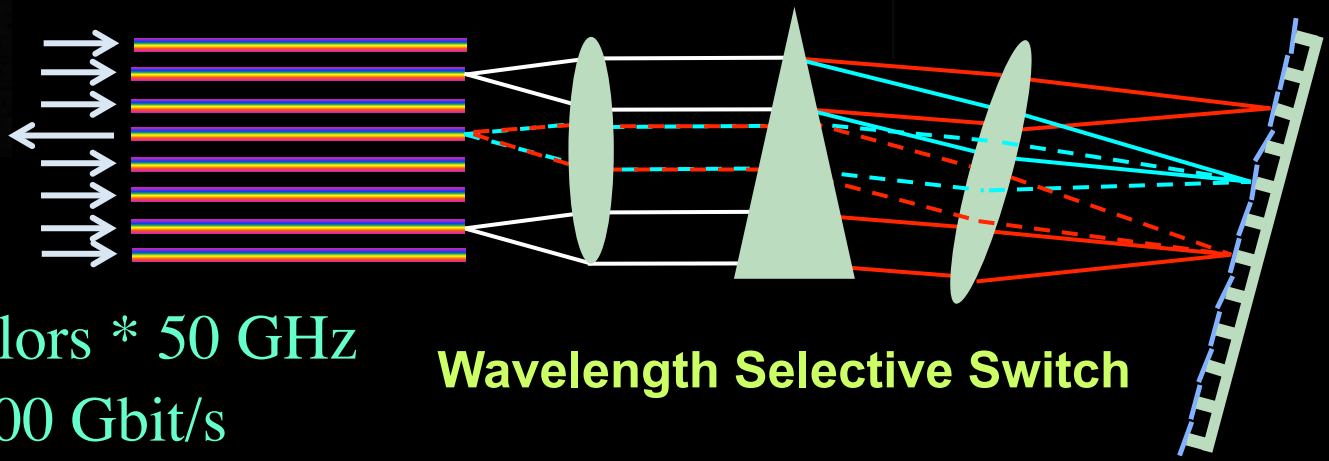

Genexis
12v
T1
T2
analoge tv
coax
internet
E1
dig. tv
E2
E3
E4
glas
voip
voip
router
switch


PoP #3
Transit
Tier 1 Networks
Tier 2 Networks
Transit
Peering
IXP
PoP #2
PoP #1
Tier 2 ISP
Transit
Transit
Tier 3 Network
(multi-homed ISP)
Tier 3 Network
(single homed ISP)
Internet users
(business, consumers, etc)

Multiple colors / Fiber







Per fiber: ~ 80-100 colors * 50 GHz

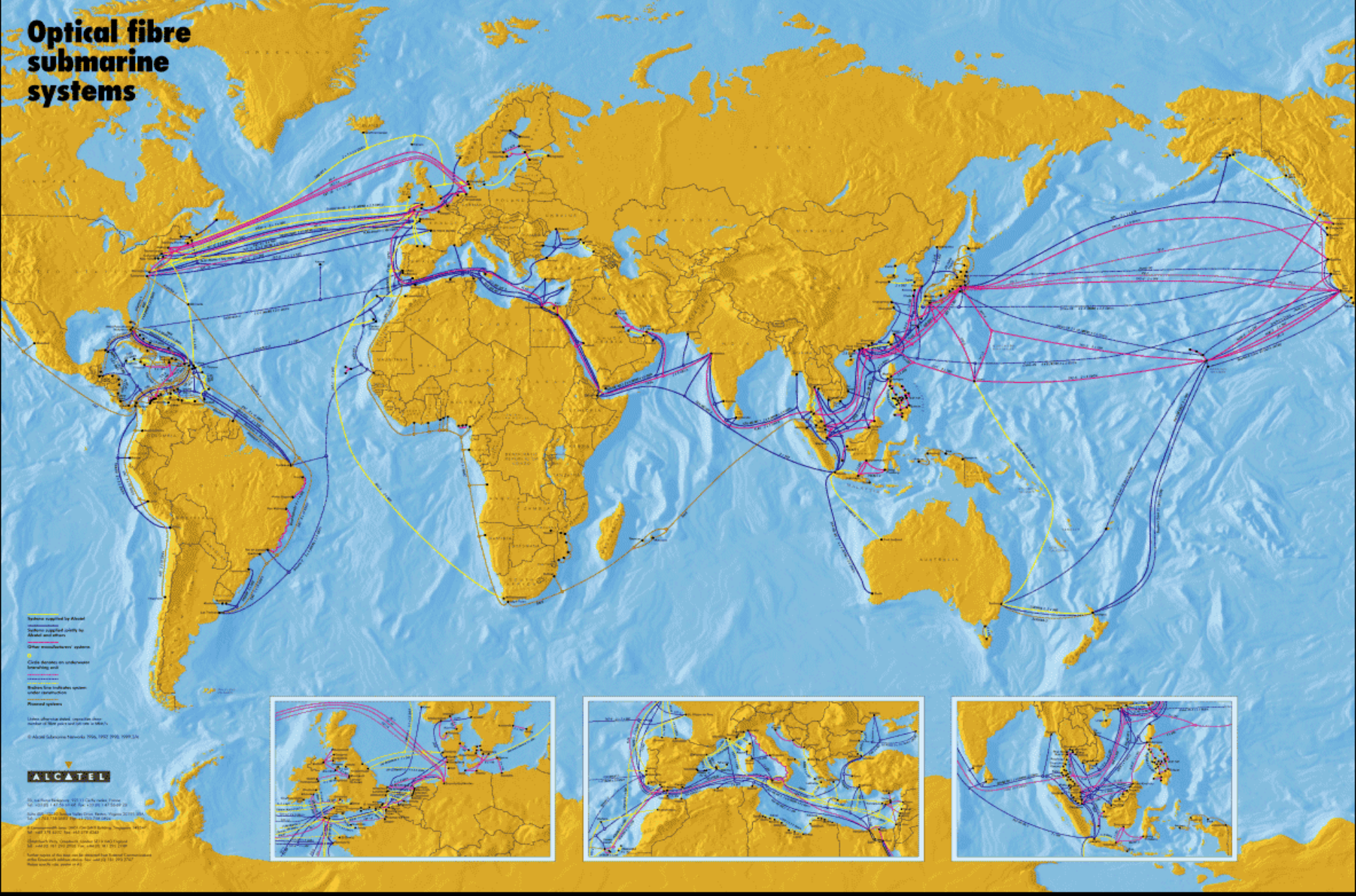
Per color: 10 – 40 – 100 Gbit/s

Max total: 10 Tbit/s = 1 Tbyte/s

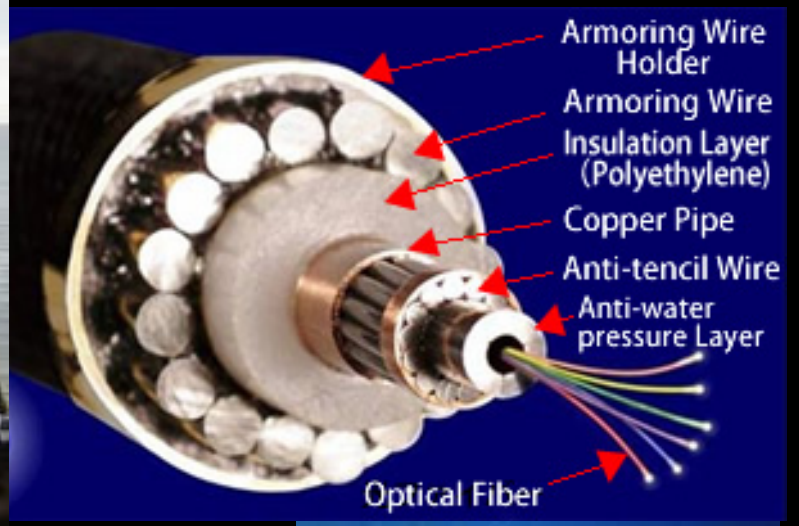
Wavelength Selective Switch

New: Hollow Fiber!

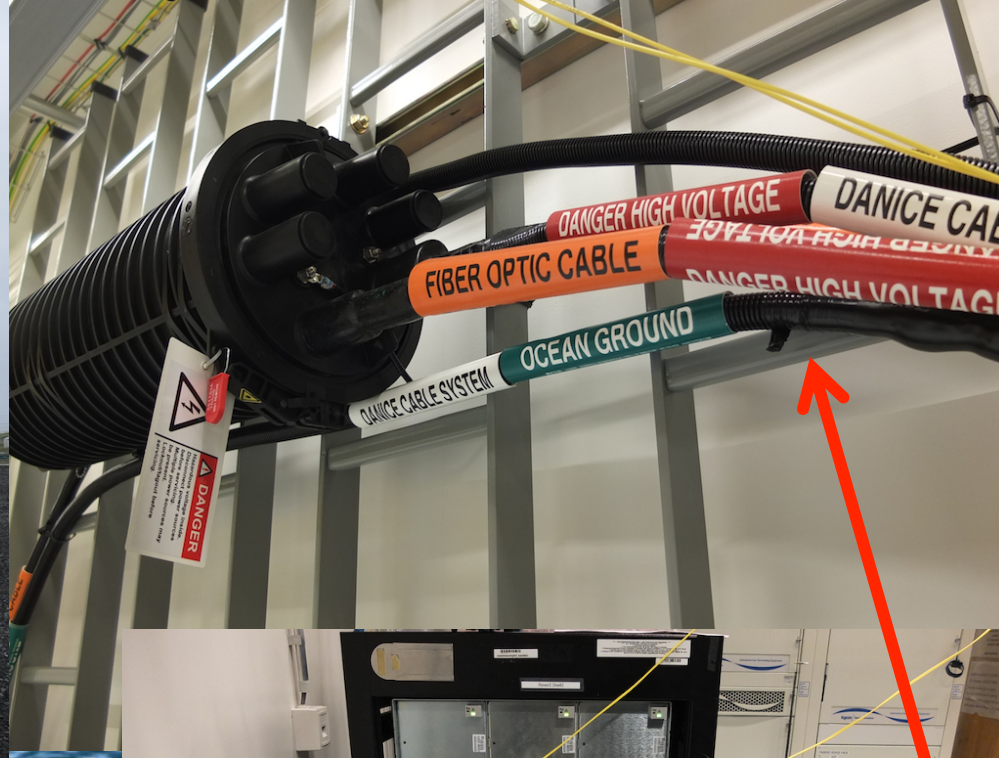
➔ less RTT!



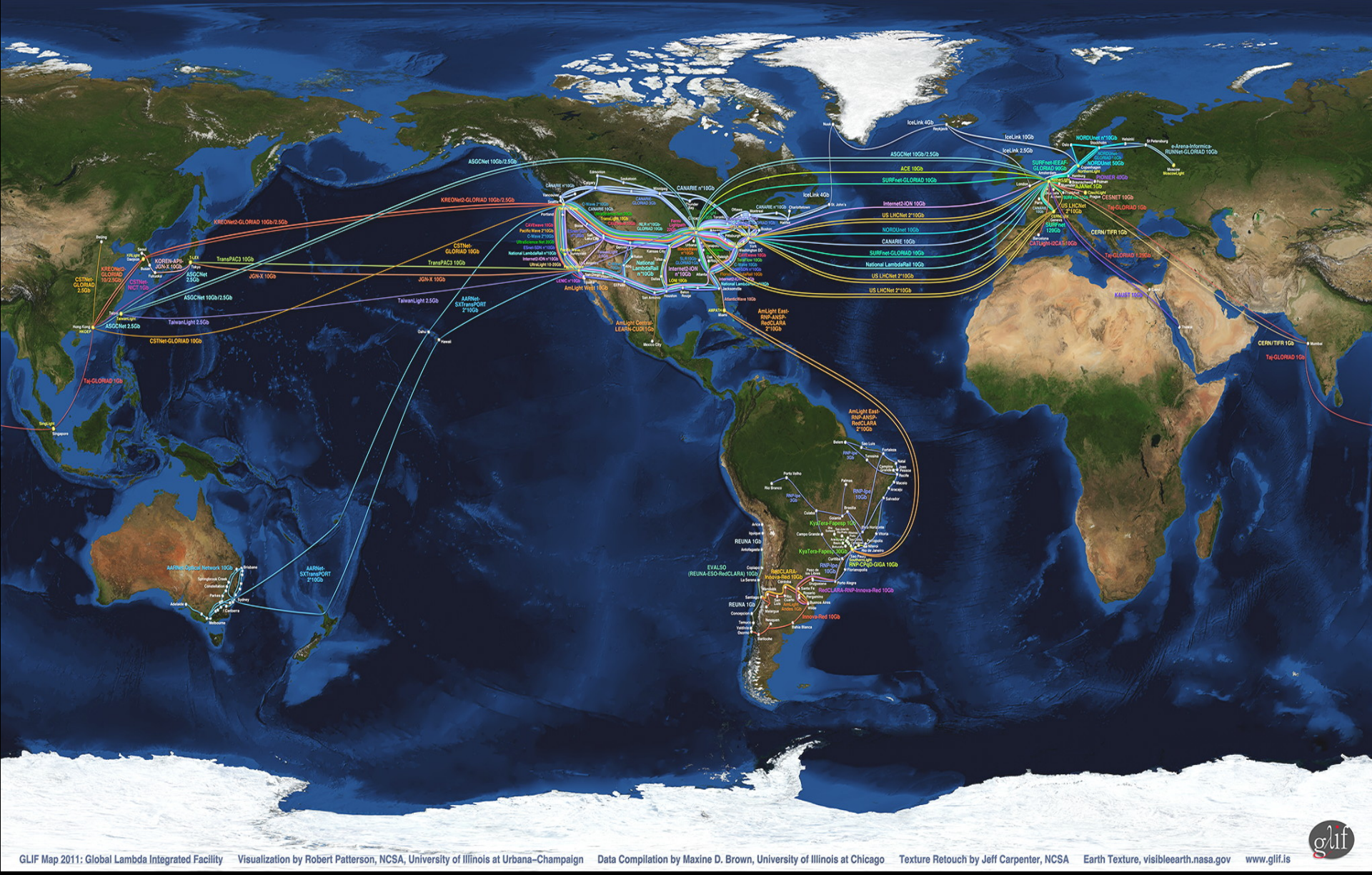
Undersea Cable System



A **cable landing station** may or may not be required, depending on whether, for example, the submarine cable requires power to power submarine repeaters or amplifiers. The voltages applied to the cables can be high **3,000 to 4,000 volts** for a typical trans-Atlantic telecommunications cable system, and 1,000 volts for a cross-channel telecommunications cable system. Submarine power cables can operate at many kilovolts: for example, the[Fenno-Skan power cable operates at 400 kV DC.]

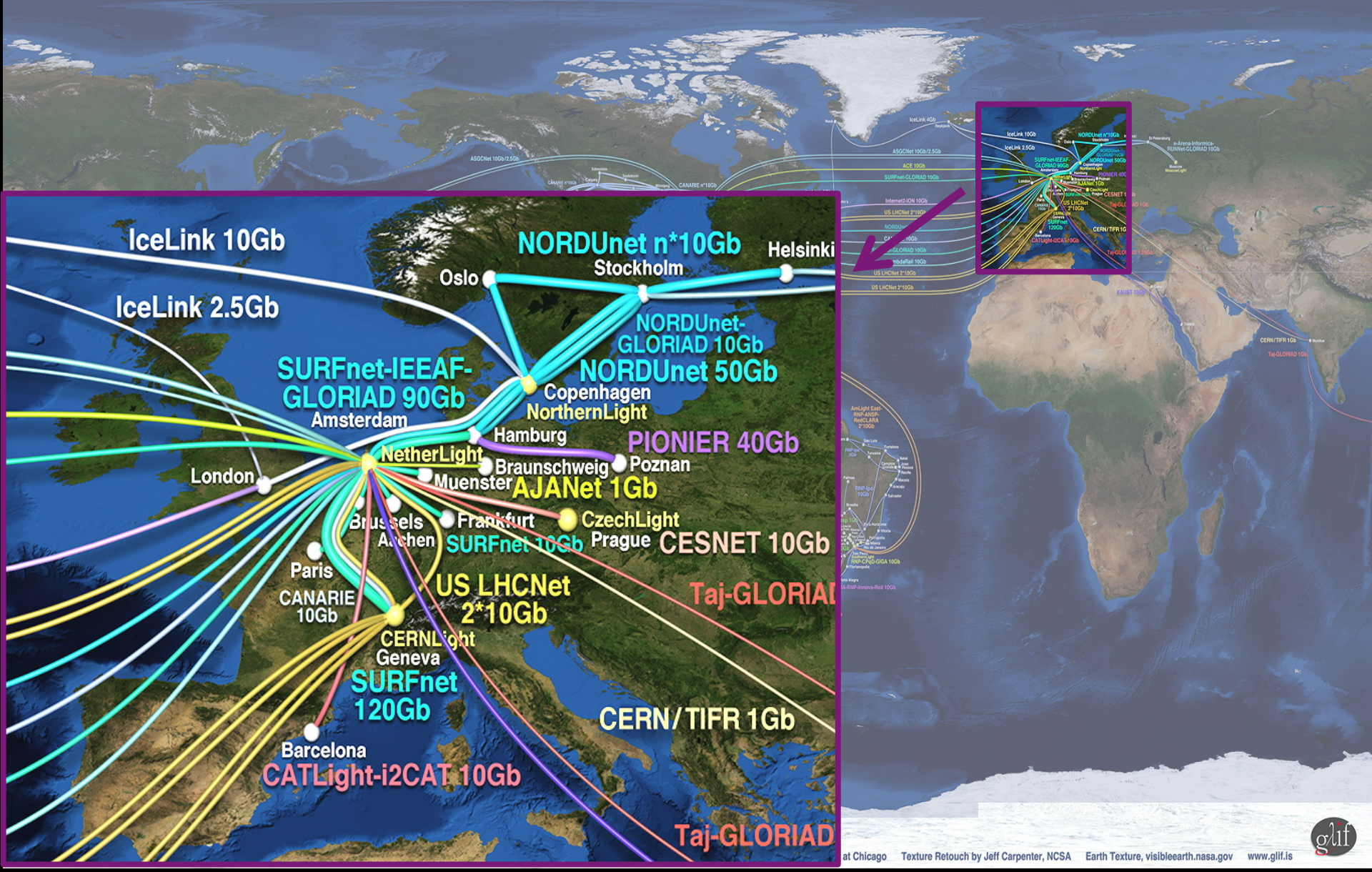


Undersea Cable HV



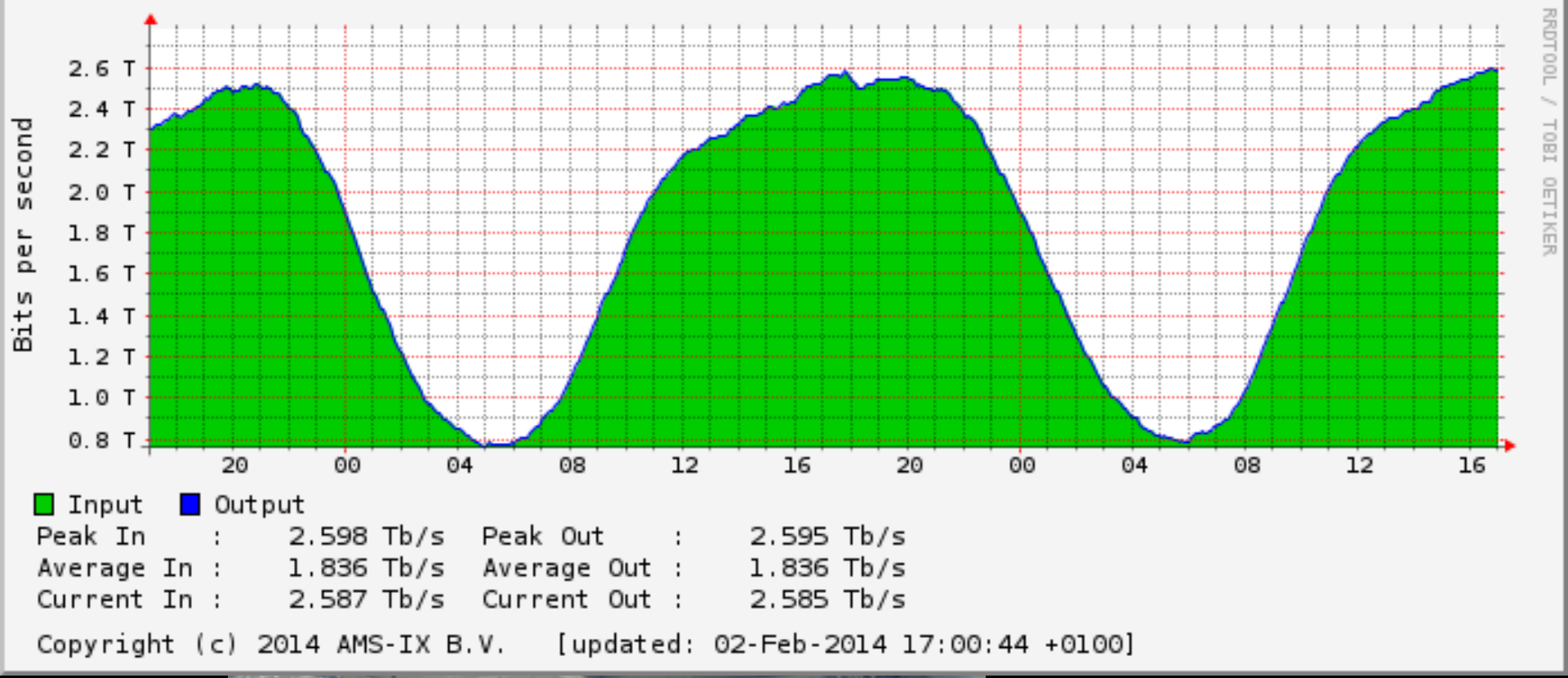
F Dijkstra, J van der Ham, P Grosso, C de Laat, “A path finding implementation for multi-layer networks”, Future Generation Computer Systems 25 (2), 142-146.

The GLIF – LightPaths around the World



F Dijkstra, J van der Ham, P Grosso, C de Laat, “A path finding implementation for multi-layer networks”, Future Generation Computer Systems 25 (2), 142-146.

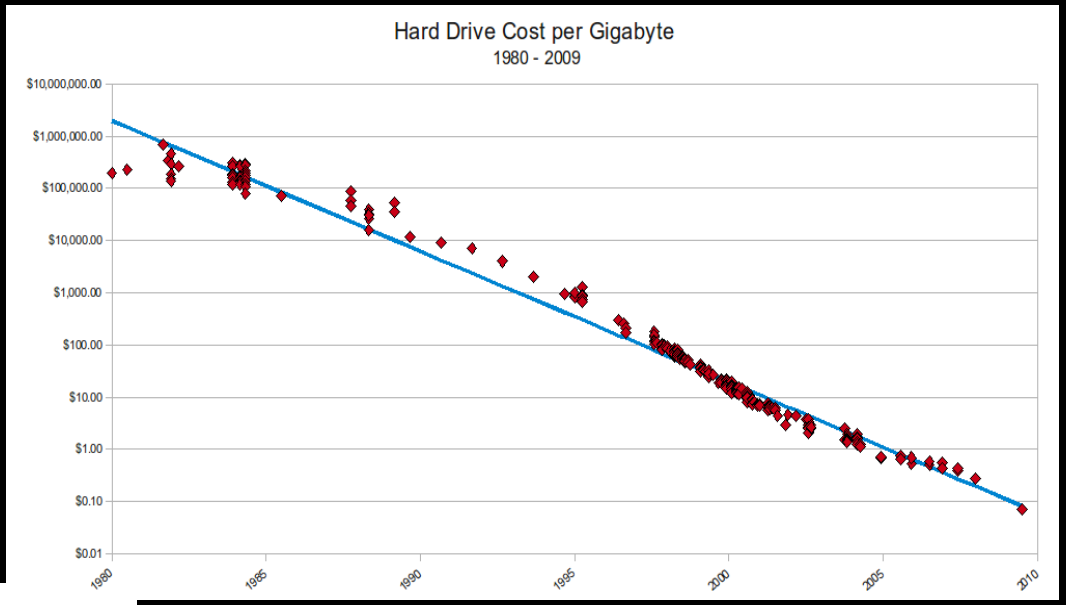
The GLIF – LightPaths around the World

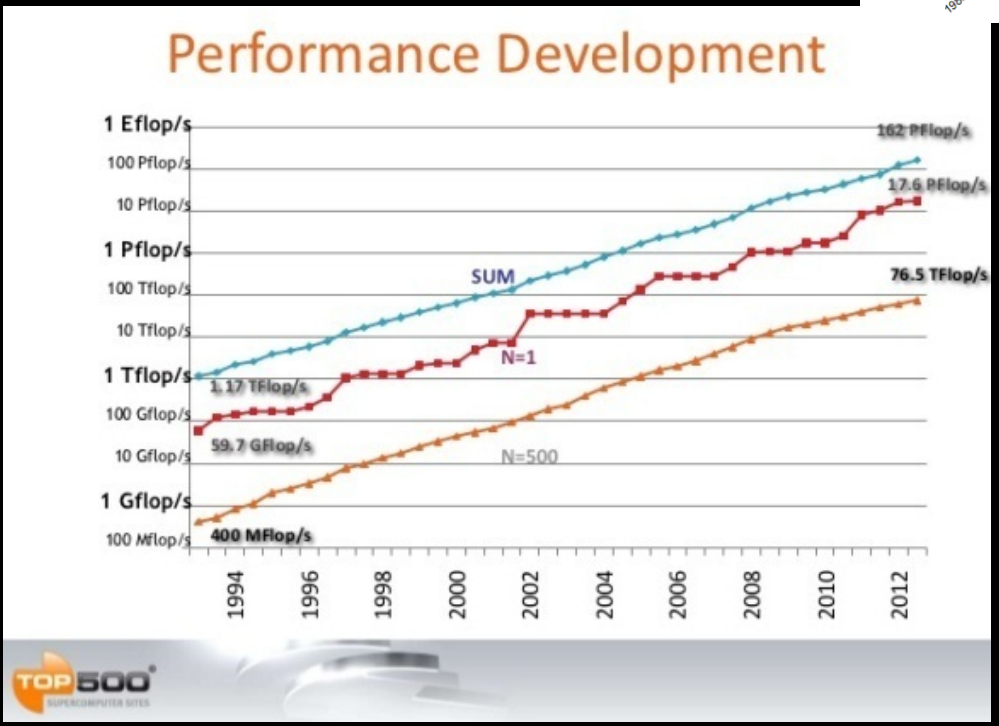


amsix
amsterdam internet exchange

Computing vs Data

Computing per unit cost has doubled roughly every 18 months.

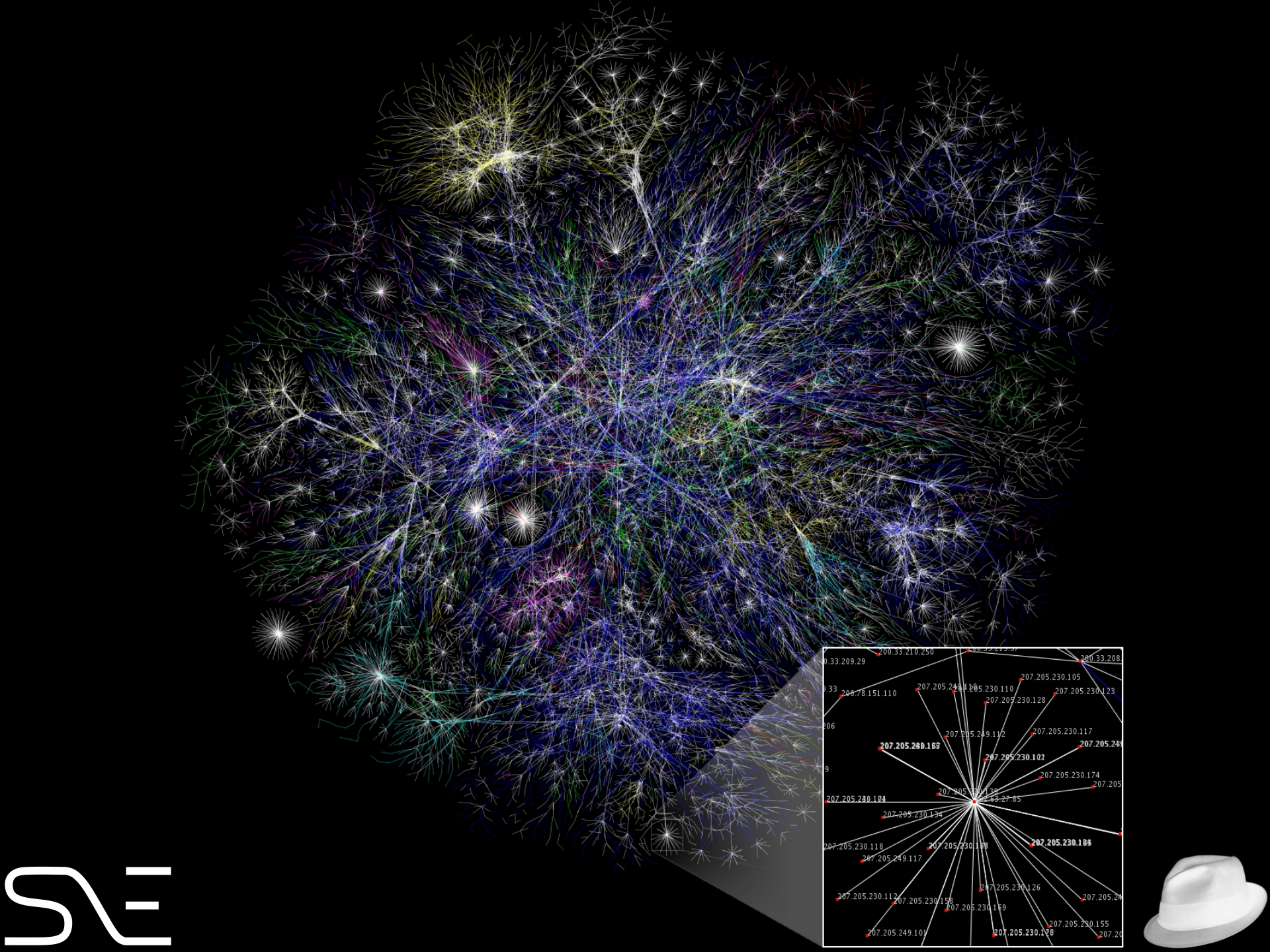




Space per unit cost has doubled roughly every 14 months.

So: data becomes exponentially uncomputable.

http://www.mkomo.com/cost-per-gigabyte


200.33.210.250
207.205.230.105
207.205.230.110
207.205.230.123
200.78.151.110
207.205.230.128
207.205.249.112
207.205.230.117
207.205.230.174
207.205.230.134
207.205.230.118
207.205.249.117
207.205.230.126
207.205.230.156
207.205.230.159
207.205.230.155
207.205.249.101

Het lek

- A series of exposés beginning June 5, 2013 revealed Internet surveillance programs such as PRISM, XKeyscore and Tempora, as well as the interception of US and European telephone metadata.

- The two principal components of Tempora are called (wikipedia)
  - "Mastering the Internet" (MTI)
  - "Global Telecoms Exploitation”
- Collate online and telephone traffic
- Data from fibre-optic cable communications.
- Data is preserved for three days, metadata for thirty days.
- By May 2012 300 GCHQ analysts and 250 NSA analysts had been assigned to sort data.[4] About 850,000 people have security clearance to access the data.
- Tempora said to include recordings of telephone calls, content of email messages, Facebook entries and personal internet history of users.
- Snowden said of Tempora that "It's not just a U.S. problem. “They [GCHQ] are worse than the U.S.”
- Dutch programs (iColumbo: http://columbo.nl/)

TEMPORA

What is XKEYSCORE?

1. DNI Exploitation System/Analytic Framework

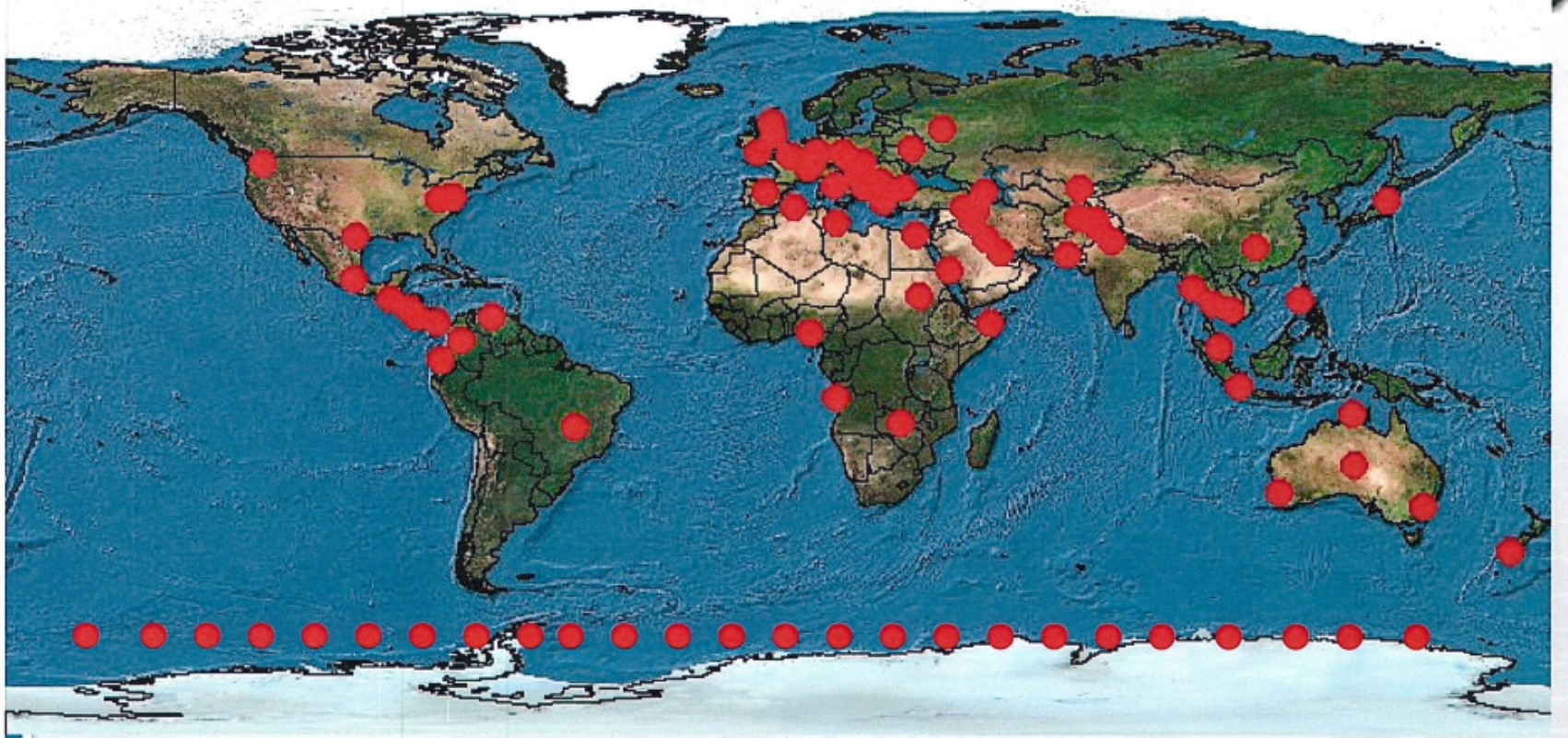
2. Performs strong (e.g. email) and soft (content) selection

3. Provides real-time target activity (tipping)

4. "Rolling Buffer" of ~3 days of ALL unfiltered data seen by XKEYSCORE:
   - Stores full-take data at the collection site – indexed by meta-data
   - Provides a series of viewers for common data types

1. Federated Query system – one query scans all sites
   - Performing full-take allows analysts to find targets that were previously unknown by mining the meta-data

Where is X-KEYSCORE?

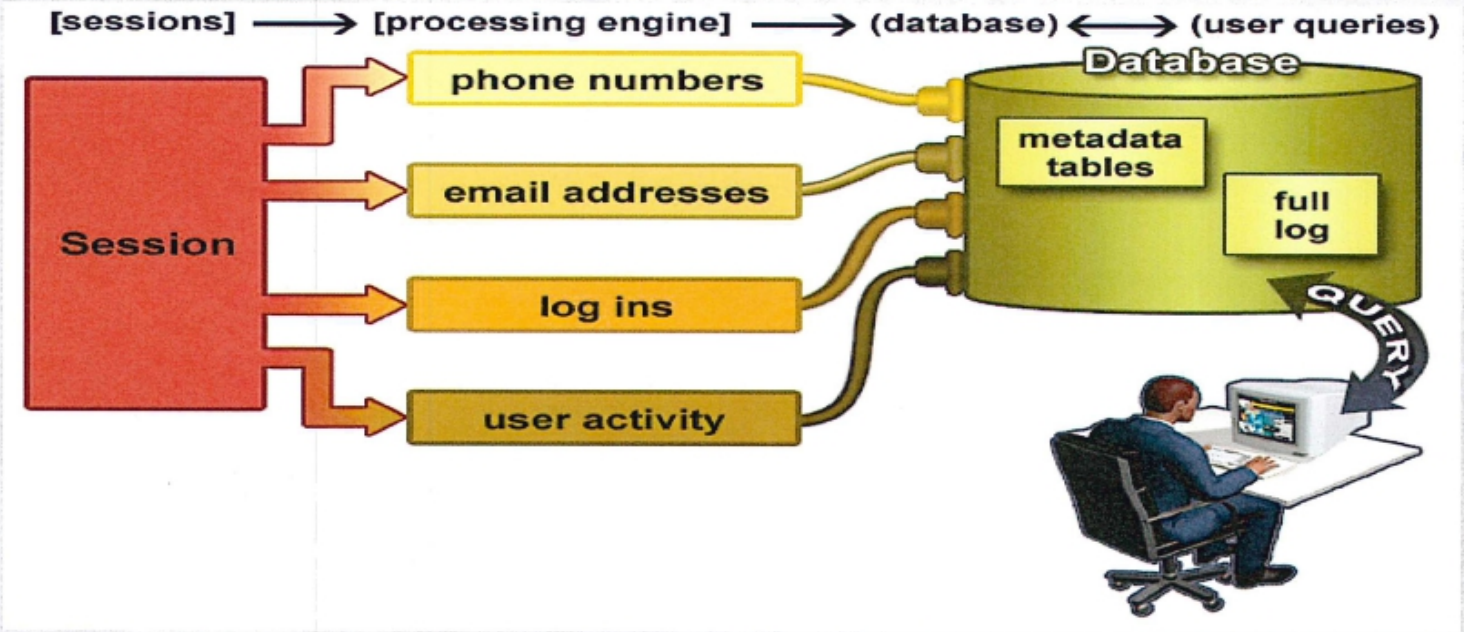


Approximately 150 sites

Over 700 servers

What XKS does with the Sessions

Plug-ins extract and index metadata into tables



Plug-ins

Plug-in	DESCRIPTION
E-mail Addresses	Indexes every E-mail address seen in a session by both username and domain
Extracted Files	Indexes every file seen in a session by both filename and extension
Full Log	Indexes every DNI session collected. Data is indexed by the standard N-tupple (IP, Port, Casenotation etc.)
HTTP Parser	Indexes the client-side HTTP traffic (examples to follow)
Phone Number	Indexes every phone number seen in a session (e.g. address book entries or signature block)
User Activity	Indexes the Webmail and Chat activity to include username, buddylist, machine specific cookies etc.

What Can Be Stored?

- Anything you wish to extract
  - Choose your metadata
  - Customizable storage times
  - Ex: HTTP Parser

[redacted]

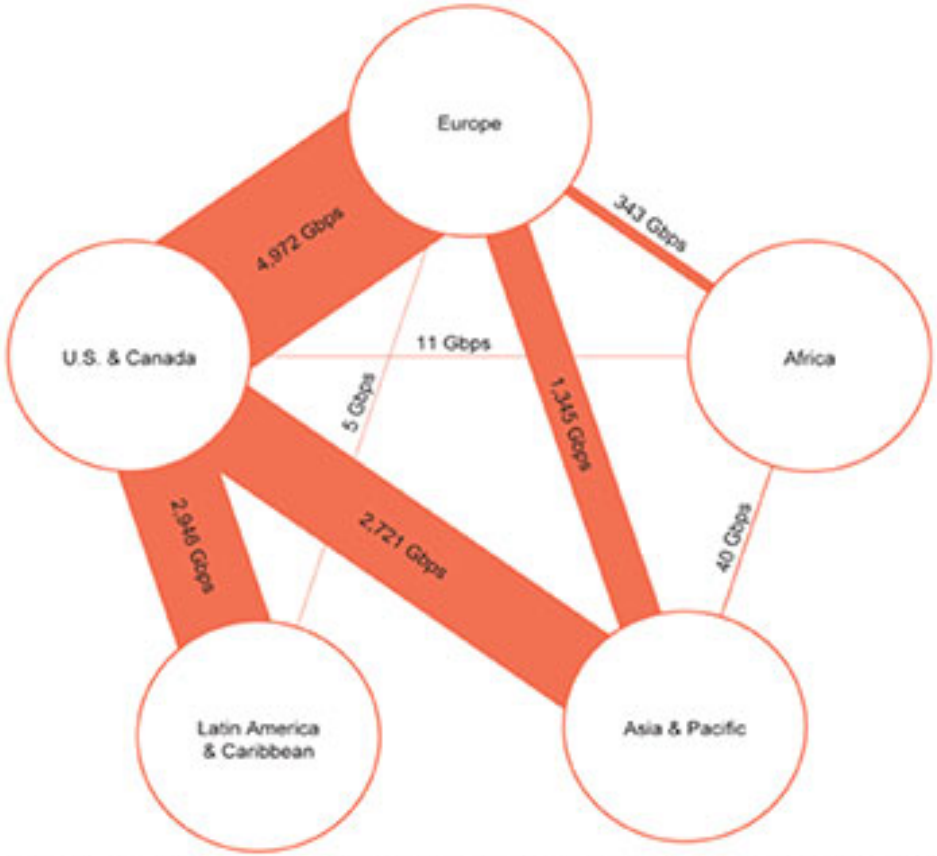
```
GET /search?hl=en&q=islamabad&meta= HTTP/1.0
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-
application/msword, application/x-shockwave-flash, */*
Referer: http://www.google.com.pk/
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: www.google.com.pk
[redacted]
Connection: keep-alive
```

No username/strong selector

(TS//SI//NF) Introduction

U.S. as World's Telecommunications Backbone

- Much of the world's communications flow through the U.S.
- A target's phone call, e-mail or chat will take the **cheapest** path, **not the physically most direct** path – you can't always predict the path.
- Your target's communications could easily be flowing into and through the U.S.



International Internet Regional Bandwidth Capacity in 2011

Source: Telegeography Research

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

Current Providers

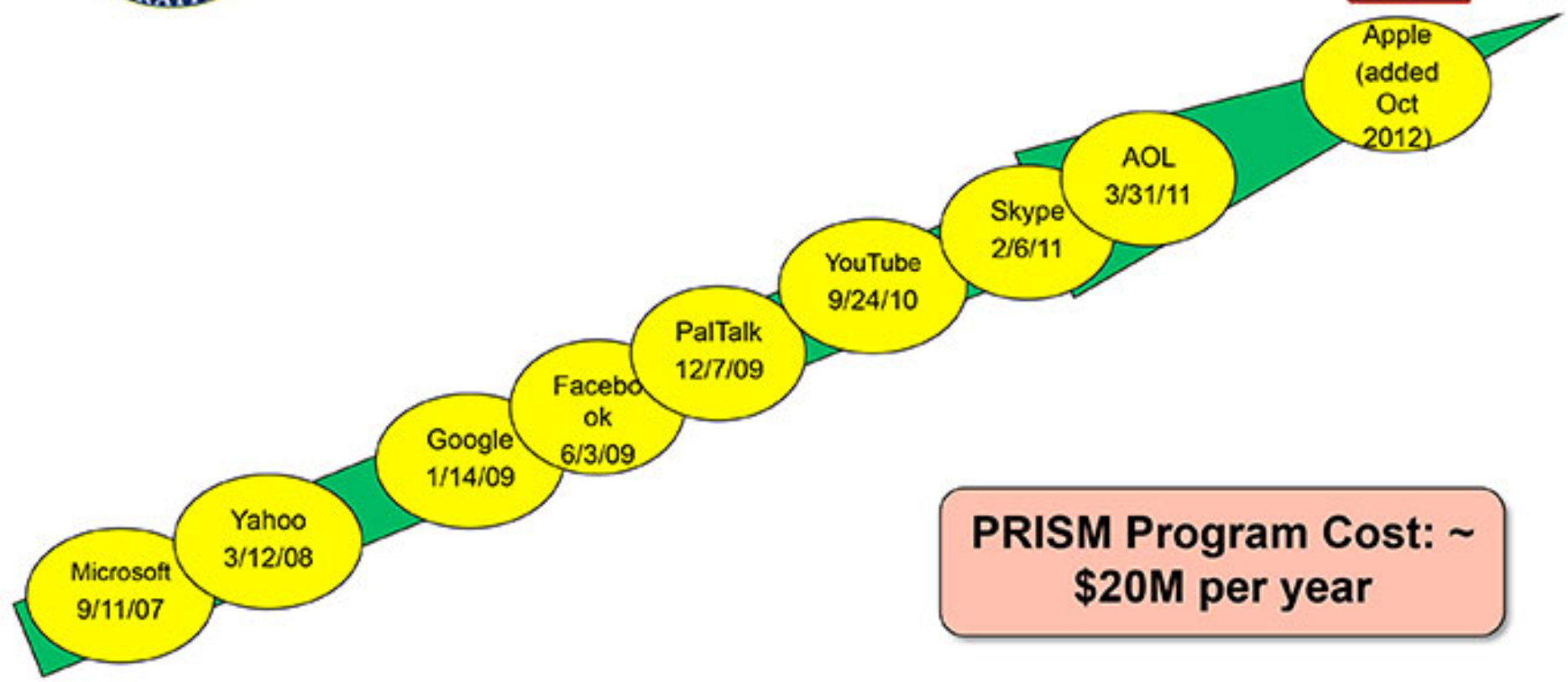
- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection (Surveillance and Stored Comms)?
It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA

(TS//SI//NF) Dates When PRISM Collection Began For Each Provider



PRISM Program Cost: ~ $20M per year


MERKEL ON THE PHONE, SHE'S VERY ANGRY
NSA
CHAPPATTE
International New York Times

Fact & Fiction

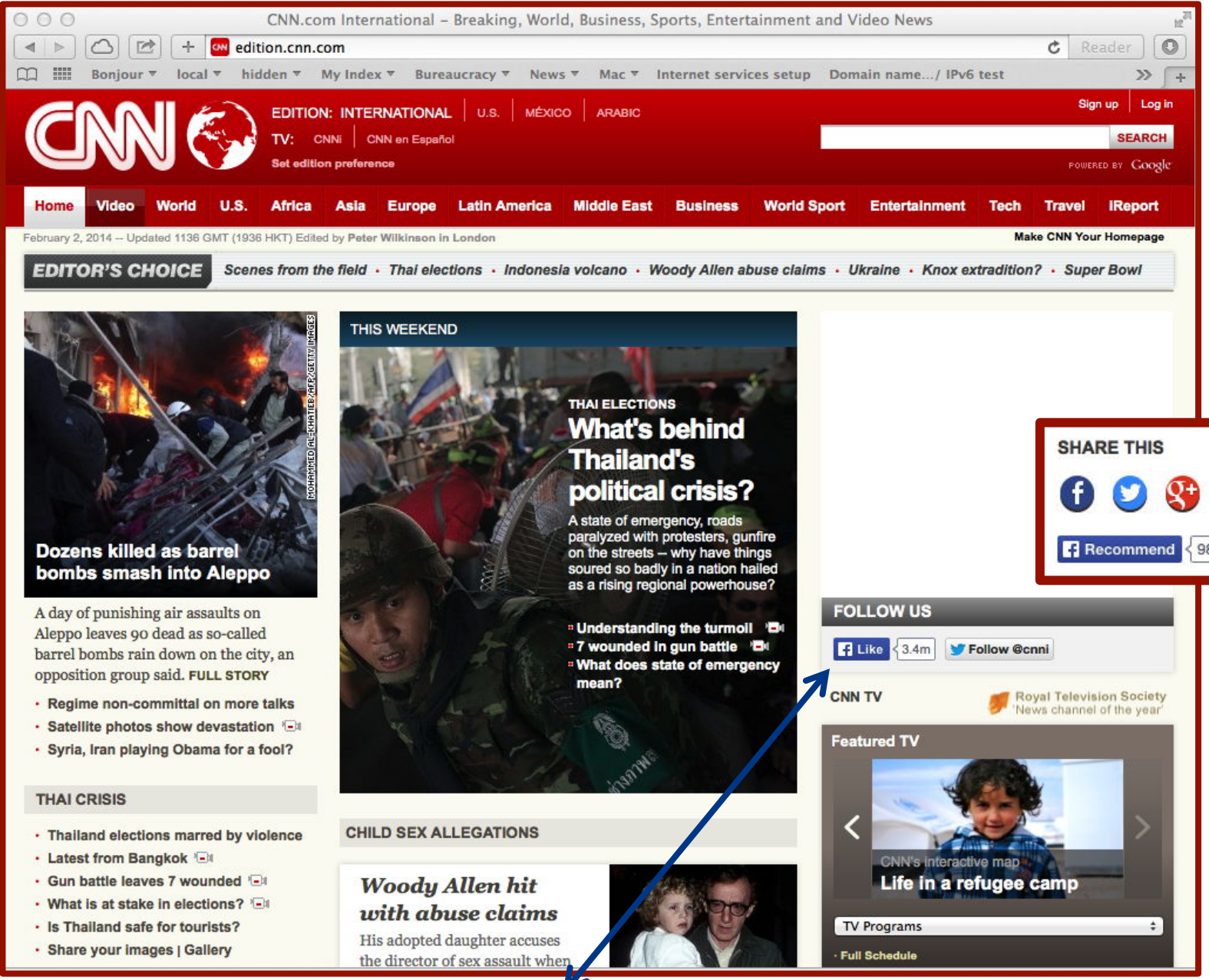
- Claims that BT pre-cooks adsl modems to send information from home networks to NSA and British Intelligence
  - http://cryptome.org/2013/12/Full-Disclosure.pdf
  - Modem connects to specific IP addresses at boot time
- Critical responses:
  - DOD uses lots of address space that is not publicly routed
    - http://blog.erratasec.com/2013/12/dod-address-space-its-not-conspiracy.html
  - See also the comment:
    "lucent uses 152.148.0.0/16 for 'management' on lots of their old big telco iron as if it was RFC-1918 space. (...)"
  - Also BT-competitor AAISP claims this is FUD:
    - https://s.aa.net.uk/1871
  - Claims: "They use DOD space because it's not internet-routable, and it's for the TR-069 (http://en.wikipedia.org/wiki/TR-069) service. This is *NOT* news."
    - http://www.bit-tech.net/news/hardware/2013/12/17/bt-back-door/1

Wat heeft dit van doen met de 2013 nationale wetenschapsquiz?

- Vraag 13: Voor een ziekte waar 1 op de 1000 mensen aan lijdt, is een 99% betrouwbare test ontwikkeld. Wat is de kans dat je ook echt ziek bent als de test dat uitwijst?

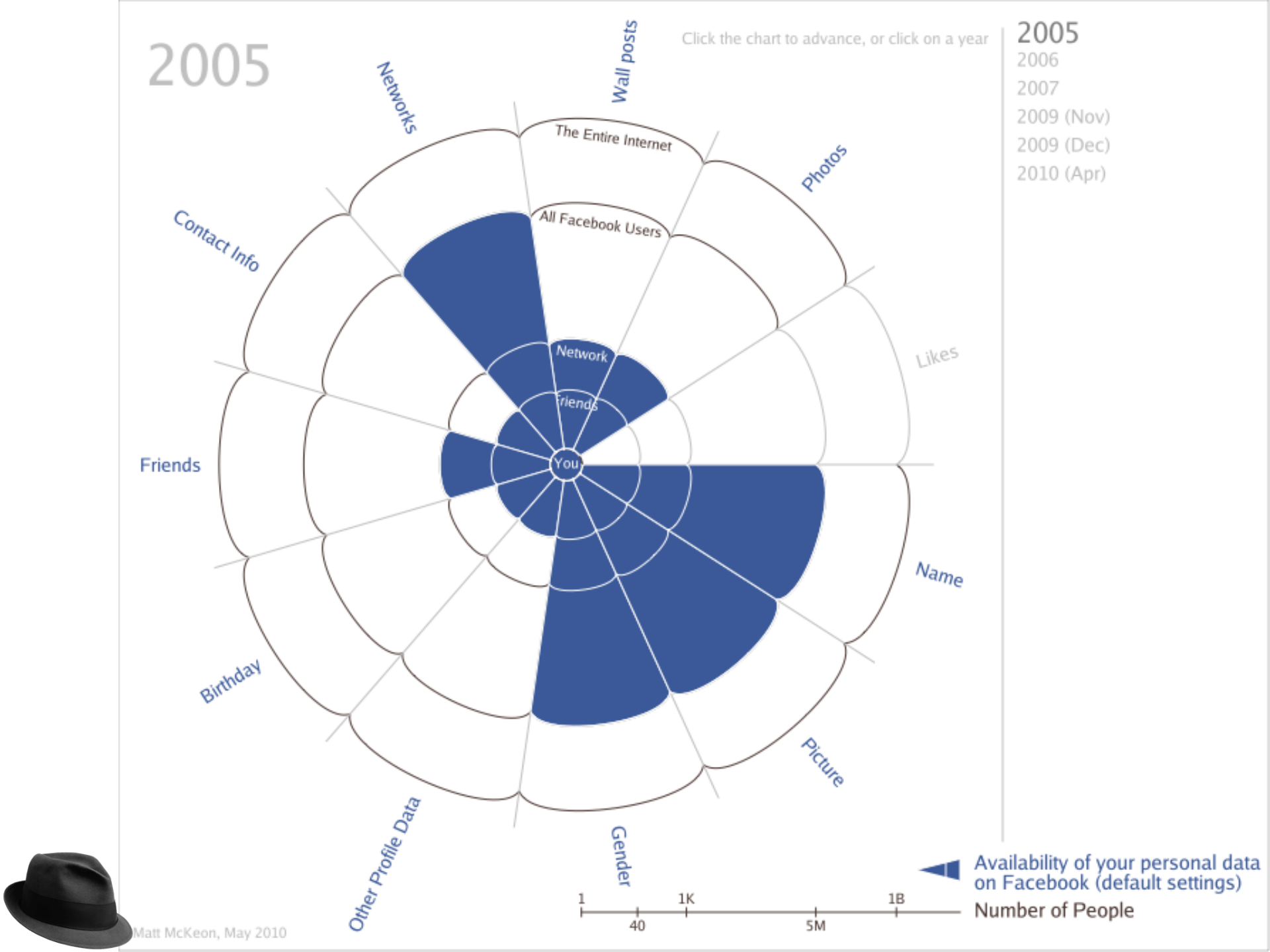
- Stel dat PRISM, Tempora, Xkeyscore, etc. in 99% van de gevallen betrouwbaar zijn en dat 1 op de 100000 subjects echt terroristen zijn…

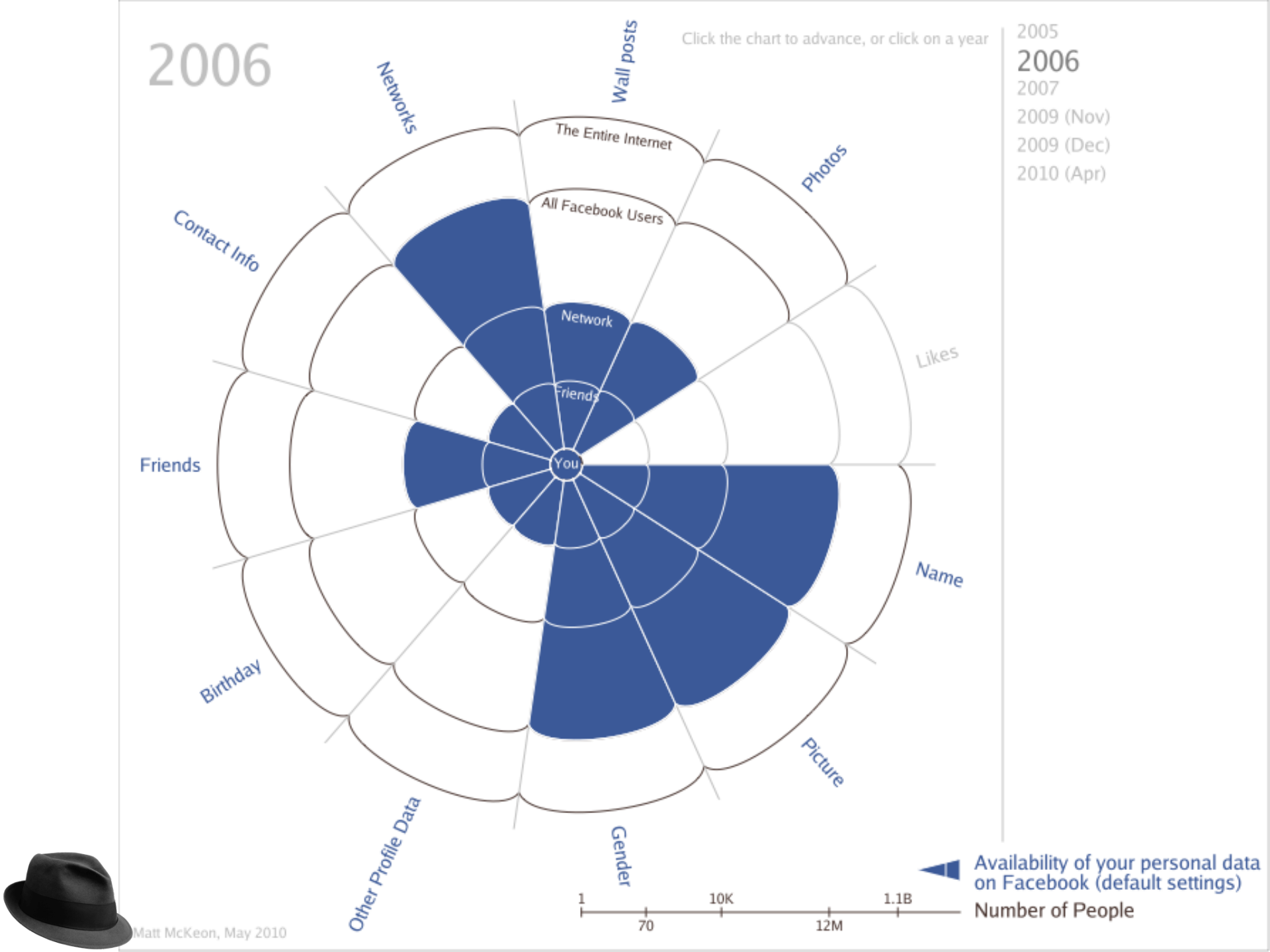
- False positives… ~1000 !

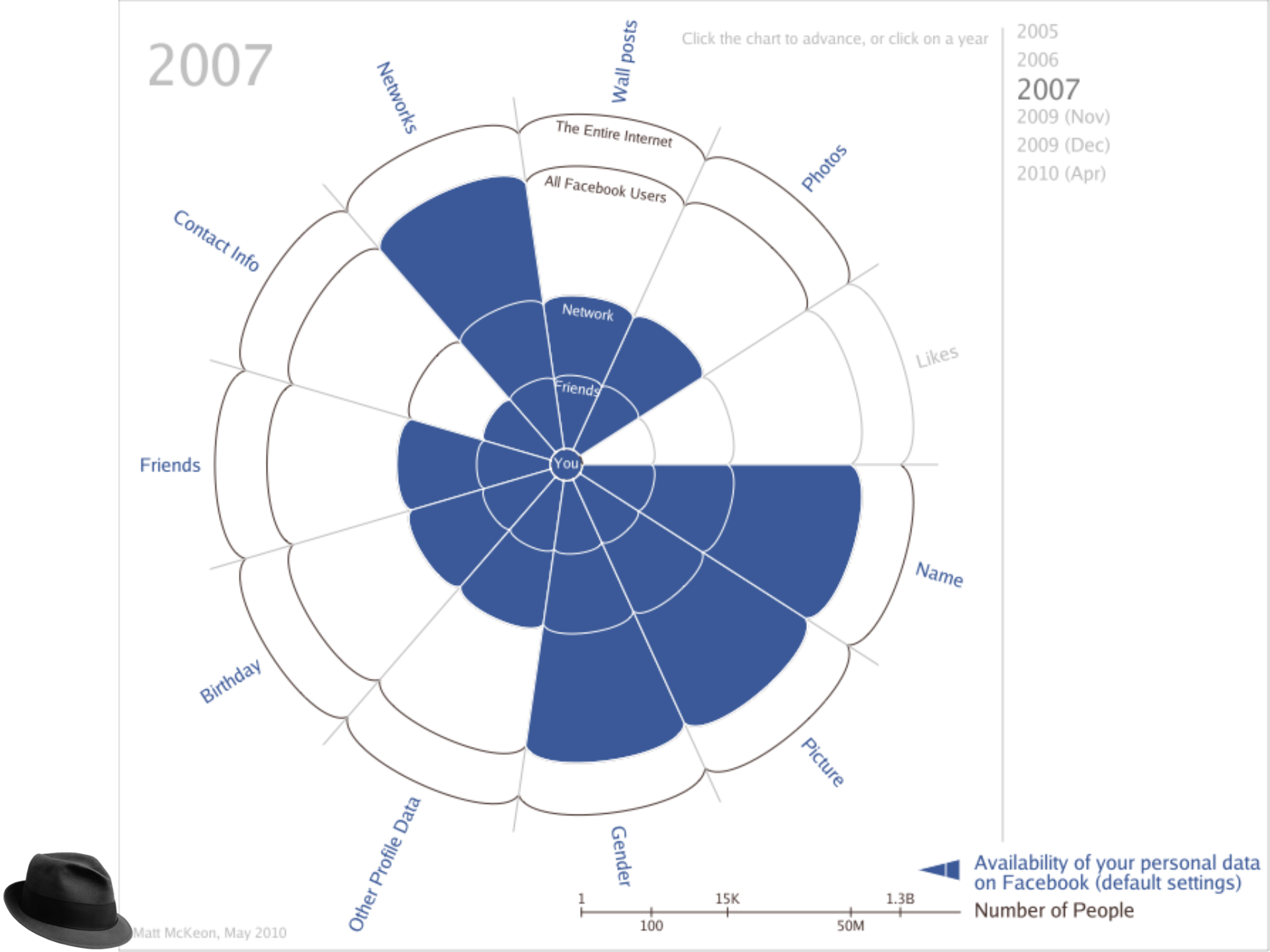


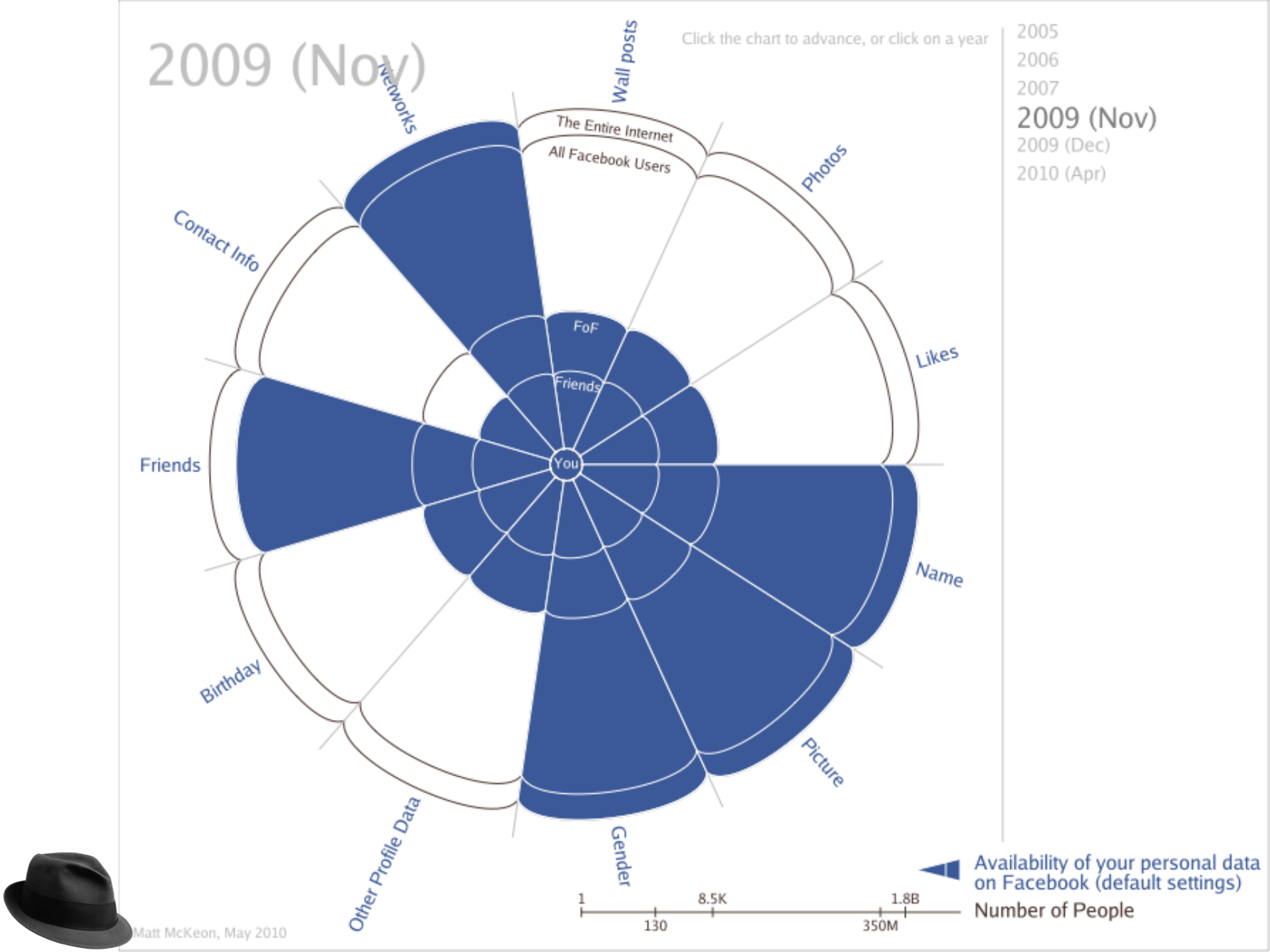
I will follow you!

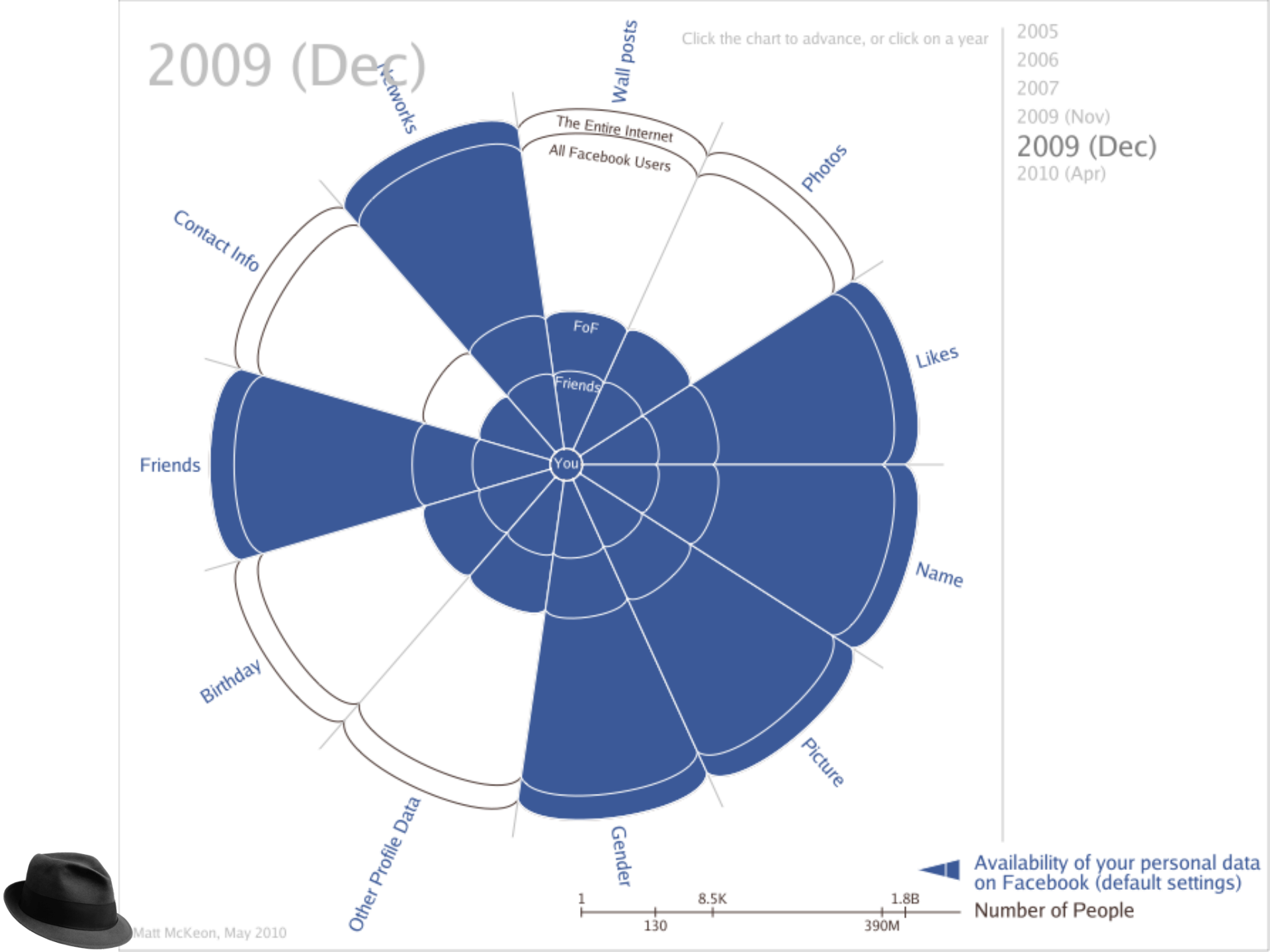
<iframe src="//www.facebook.com/plugins/like.php?href=http%3A%2F%2Fwww.facebook.com%2Fcnninternational&send=false&layout=button_count&width=450&show_faces=false&action=like&colorscheme=light&font=arial&height=21" …></iframe>

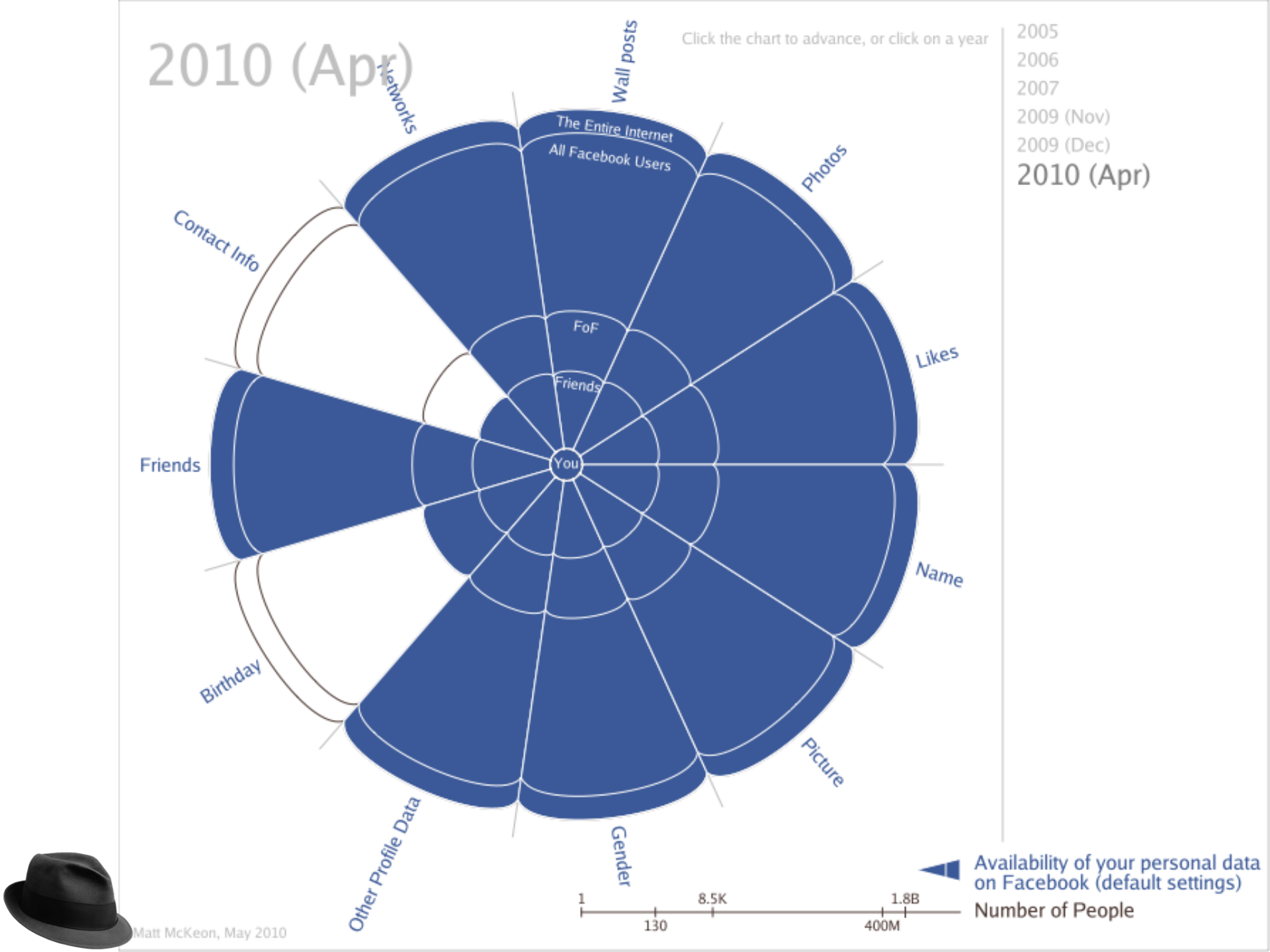

2005
Click the chart to advance, or click on a year
2005
2006
2007
2009 (Nov)
2009 (Dec)
2010 (Apr)
Networks
Wall posts
Photos
Contact Info
Likes
Friends
Name
Birthday
Picture
Other Profile Data
Gender
The Entire Internet
All Facebook Users
Network
Friends
You
Availability of your personal data on Facebook (default settings)
1
40
1K
5M
1B
Number of People
Matt McKeon, May 2010


2006
Click the chart to advance, or click on a year
2005
2006
2007
2009 (Nov)
2009 (Dec)
2010 (Apr)
Networks
Wall posts
Photos
Likes
Name
Picture
Gender
Other Profile Data
Birthday
Friends
Contact Info
The Entire Internet
All Facebook Users
Network
Friends
You
Availability of your personal data on Facebook (default settings)
1
70
10K
12M
1.1B
Number of People
Matt McKeon, May 2010


2007
Click the chart to advance, or click on a year
2005
2006
2007
2009 (Nov)
2009 (Dec)
2010 (Apr)
Networks
Wall posts
Photos
Likes
Name
Picture
Gender
Other Profile Data
Birthday
Friends
Contact Info
The Entire Internet
All Facebook Users
Network
Friends
You
Availability of your personal data on Facebook (default settings)
1
100
15K
50M
1.3B
Number of People
Matt McKeon, May 2010


2009 (Nov)
Click the chart to advance, or click on a year
2005
2006
2007
2009 (Nov)
2009 (Dec)
2010 (Apr)
Networks
Wall posts
Photos
Likes
Name
Picture
Gender
Other Profile Data
Birthday
Friends
Contact Info
The Entire Internet
All Facebook Users
FoF
Friends
You
Availability of your personal data on Facebook (default settings)
1
8.5K
1.8B
130
350M
Number of People
Matt McKeon, May 2010

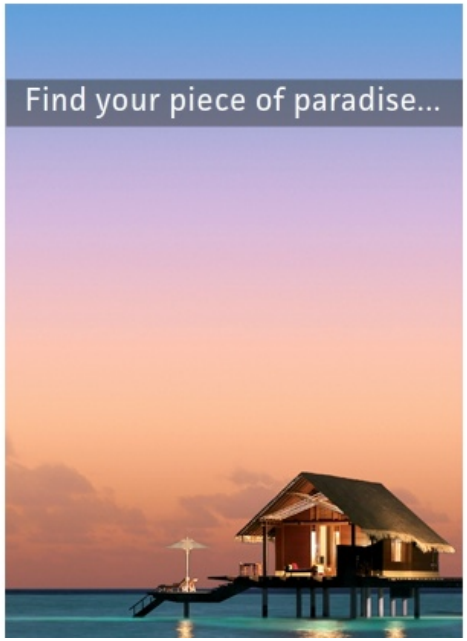

2009 (Dec)
Click the chart to advance, or click on a year
2005
2006
2007
2009 (Nov)
2009 (Dec)
2010 (Apr)
Networks
Wall posts
Photos
Likes
Name
Picture
Gender
Other Profile Data
Birthday
Friends
Contact Info
The Entire Internet
All Facebook Users
FoF
Friends
You
Availability of your personal data on Facebook (default settings)
1
8.5K
1.8B
130
390M
Number of People
Matt McKeon, May 2010


2010 (Apr)
Click the chart to advance, or click on a year
2005
2006
2007
2009 (Nov)
2009 (Dec)
2010 (Apr)
Networks
Wall posts
Photos
Likes
Name
Picture
Gender
Other Profile Data
Birthday
Friends
Contact Info
The Entire Internet
All Facebook Users
FoF
Friends
You
Availability of your personal data on Facebook (default settings)
1
8.5K
1.8B
130
400M
Number of People
Matt McKeon, May 2010

WIRED

You are Facebook's product, not customer

TECHNOLOGY / 21 SEPTEMBER 11 / by OLIVIA SOLON

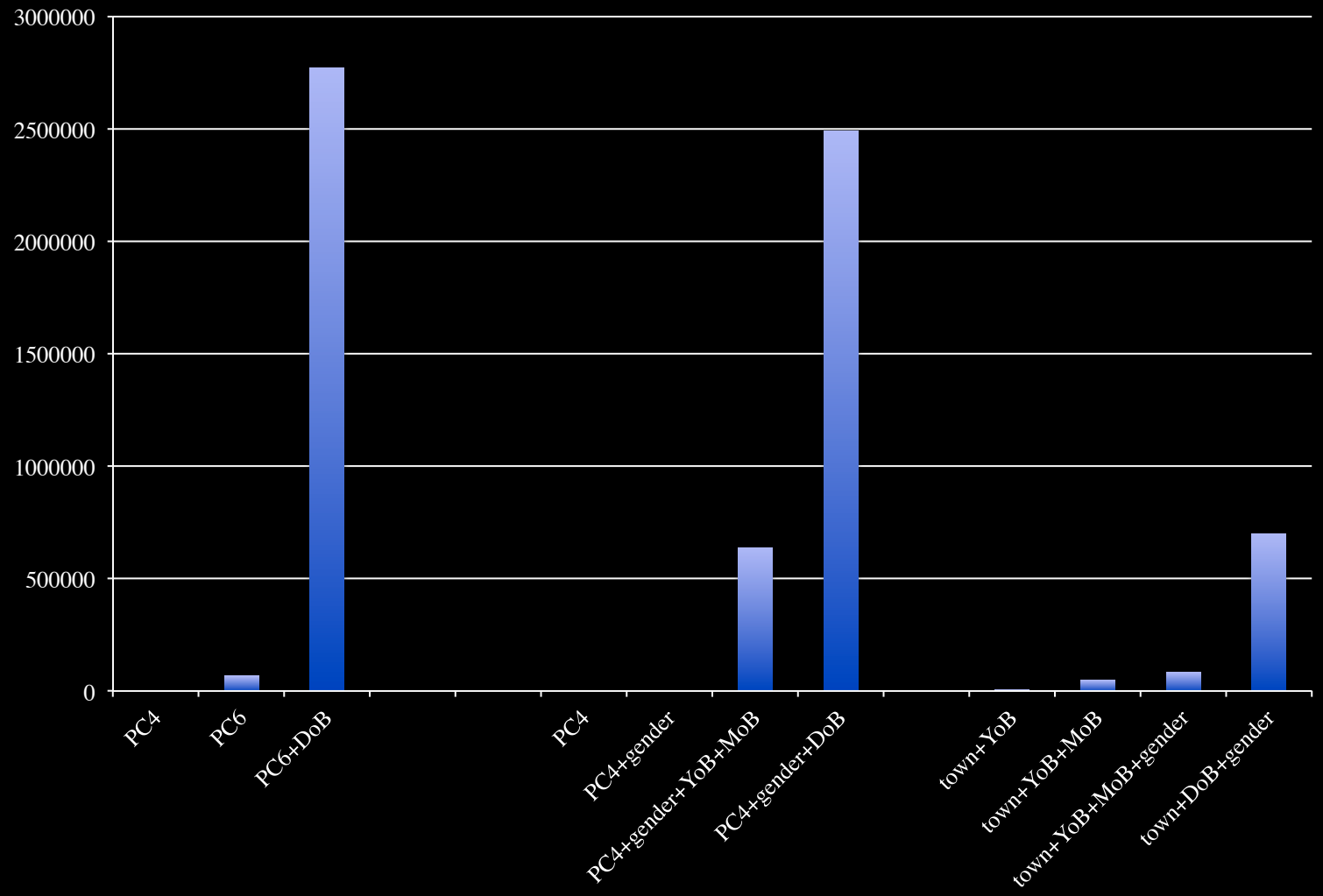


People need to understand that they are the product of Facebook and not the customer, according to media theorist and writer Douglas Rushkoff.

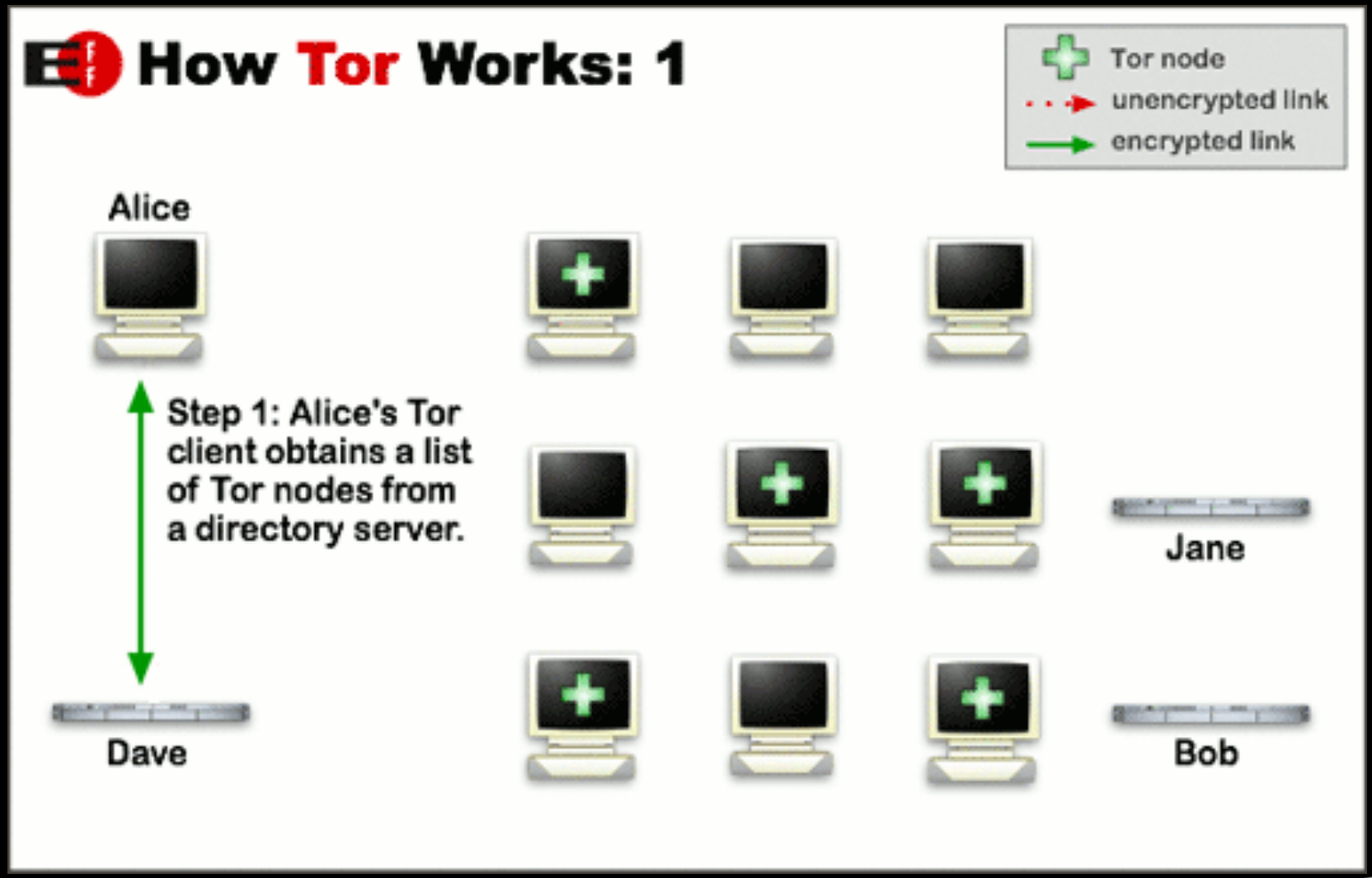
Speaking at the inaugural Hello Etsy conference in Berlin, the author of *Program or Be Programmed* said: "Ask a kid what Facebook is for and they'll answer 'it's there to help me make friends'. Facebook's boardroom isn't talking about how to make Johnny more friends. It's talking about how to monetise Johnnny's social graph."

Flickr.com/designbyfront

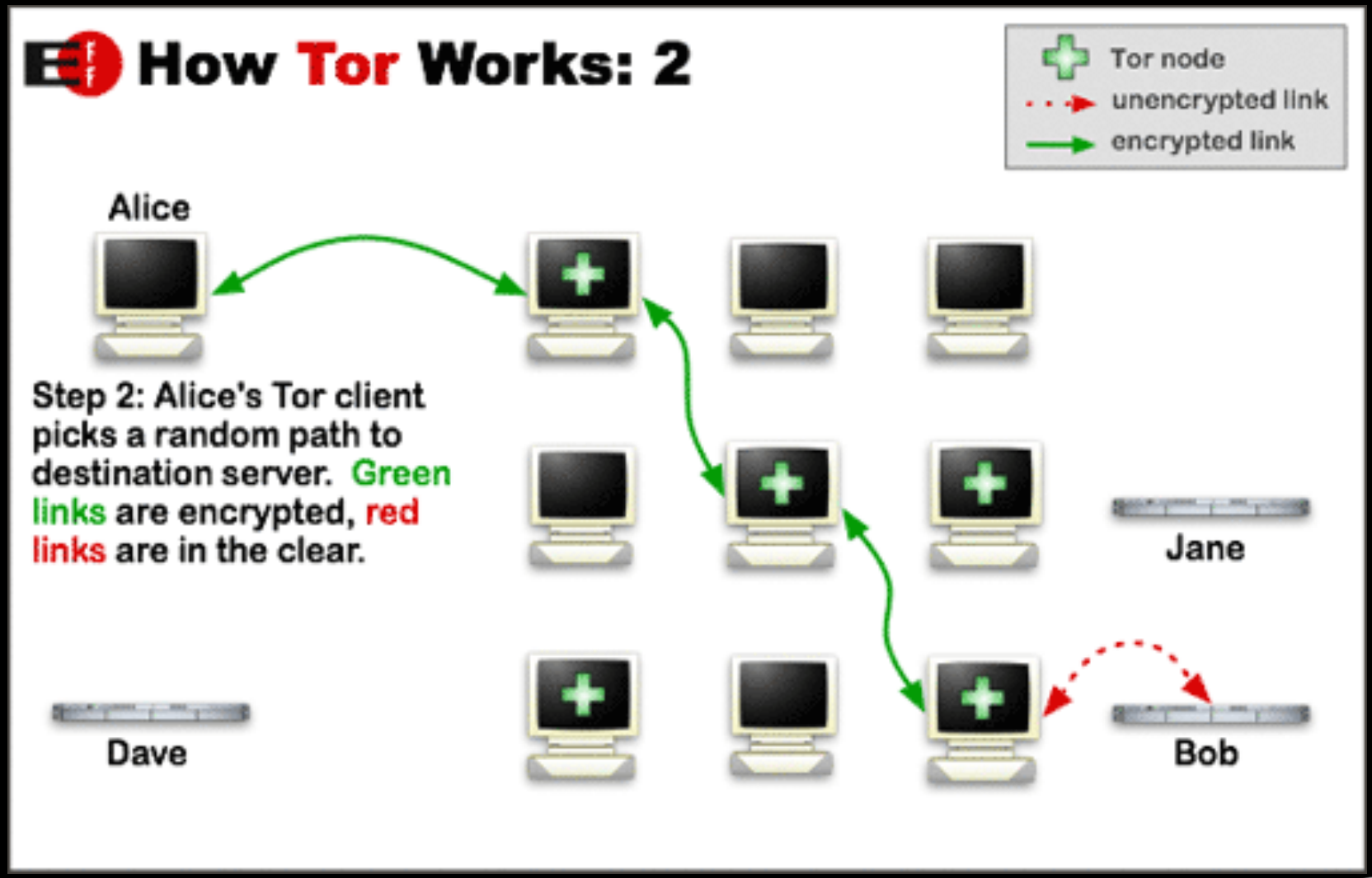
Thesis Matthijs Koot



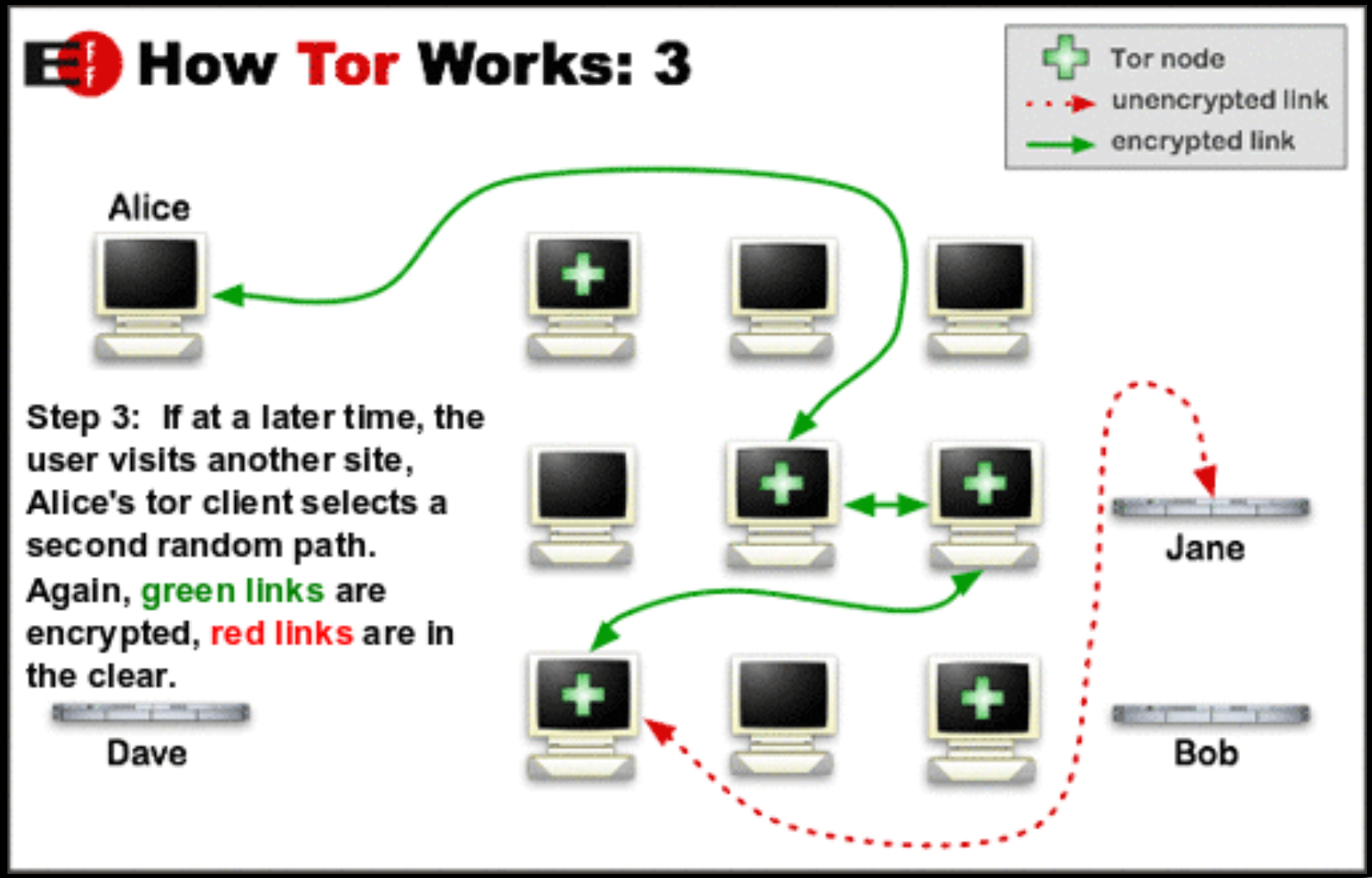
TOR: third-generation onion routing project of the U.S. Naval Research Laboratory.



TOR: third-generation onion routing project of the U.S. Naval Research Laboratory.



TOR: third-generation onion routing project of the U.S. Naval Research Laboratory.



Losse opmerkingen

- Lang niet iedereen is interessant ;-)
- False positives desastreus
- Het Internet vergeet niet
- Asymtotisch verlies aan privacy
- Proberen te verdwijnen valt net zo goed op!
- Regeringen kunnen eng zijn, vergeet industrie niet!
- NSA candy store:
  - http://en.wikipedia.org/wiki/NSA_ANT_catalog

Q & A

SPUI25
Academisch-cultureel centrum