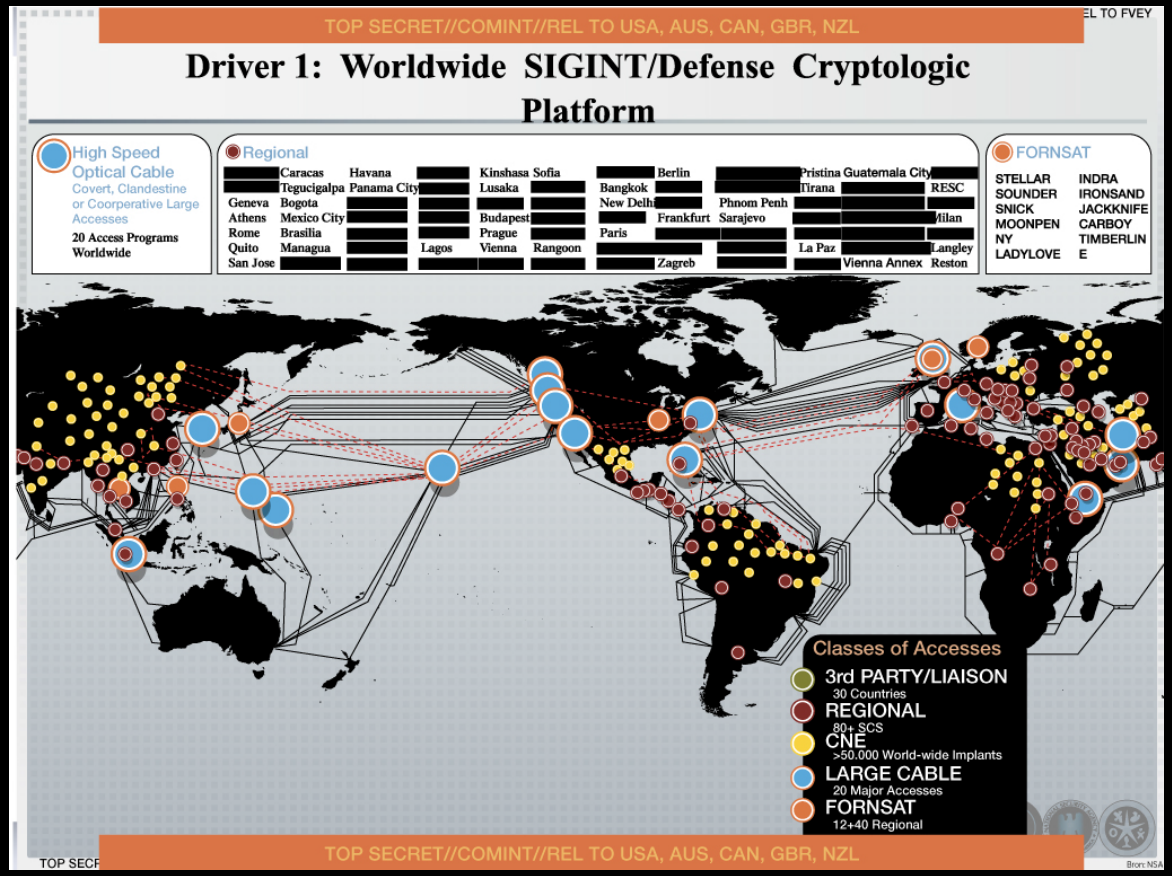
IXmaps.ca

Making mass internet surveillance visible



Andrew Clement

Fac. of Information, Univ. of Toronto

Big Data Surveillance, Snowden Archive projects

http://IXmaps.ca http://iprp.ischool.utoronto.ca/

Resisting surveillance

'kræfterne bag'

PROSA, Copenhagen

Sept. 30, 2016

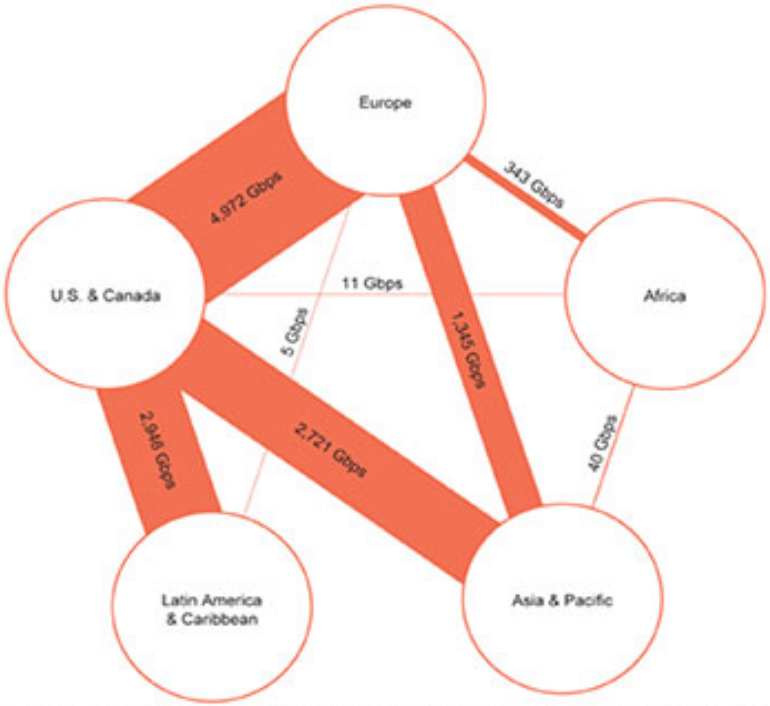
Take advantage of routing bias

TOP SECRET//SI//ORCON//NOFORN

(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.

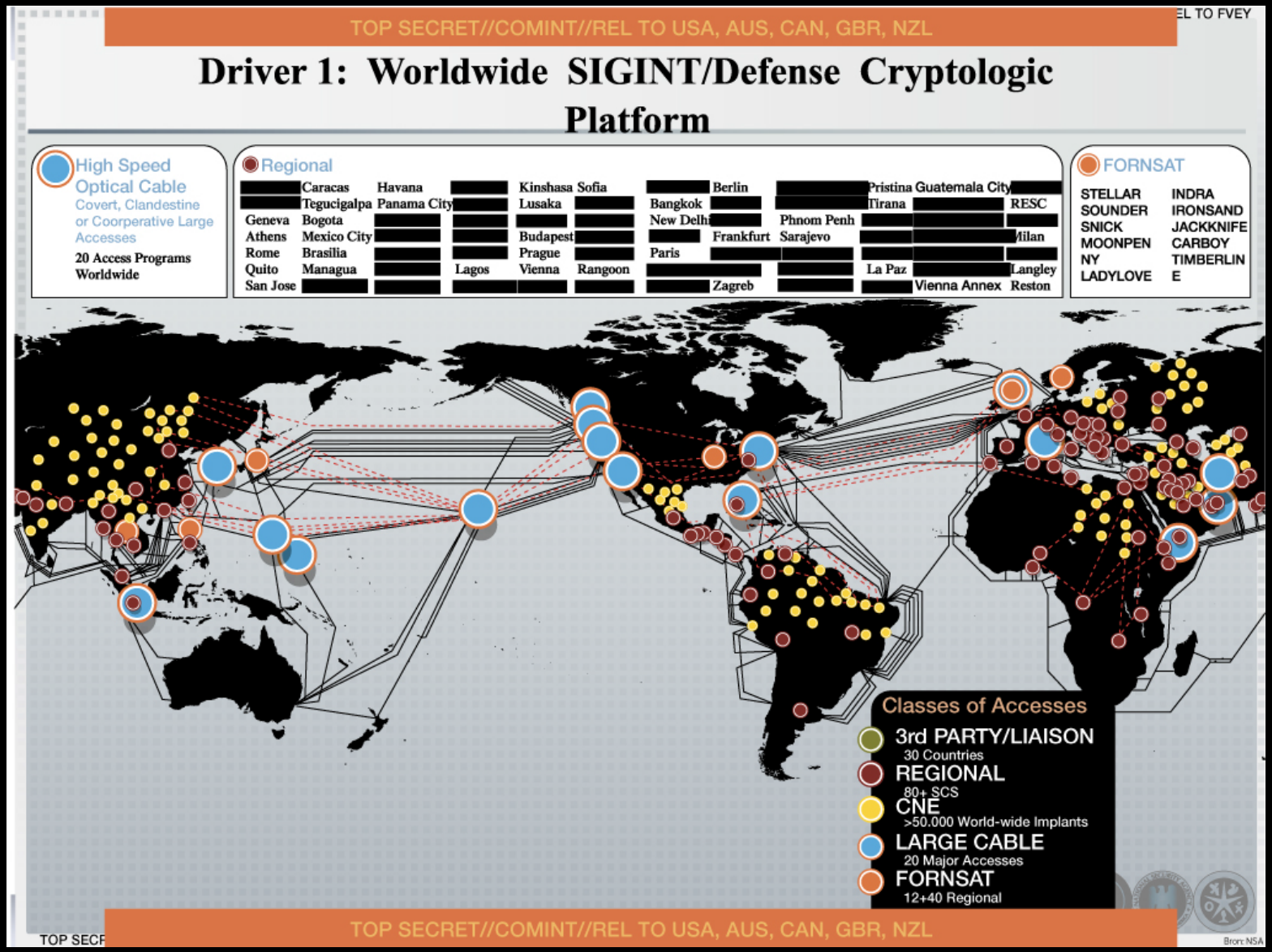


International Internet Regional Bandwidth Capacity in 2011

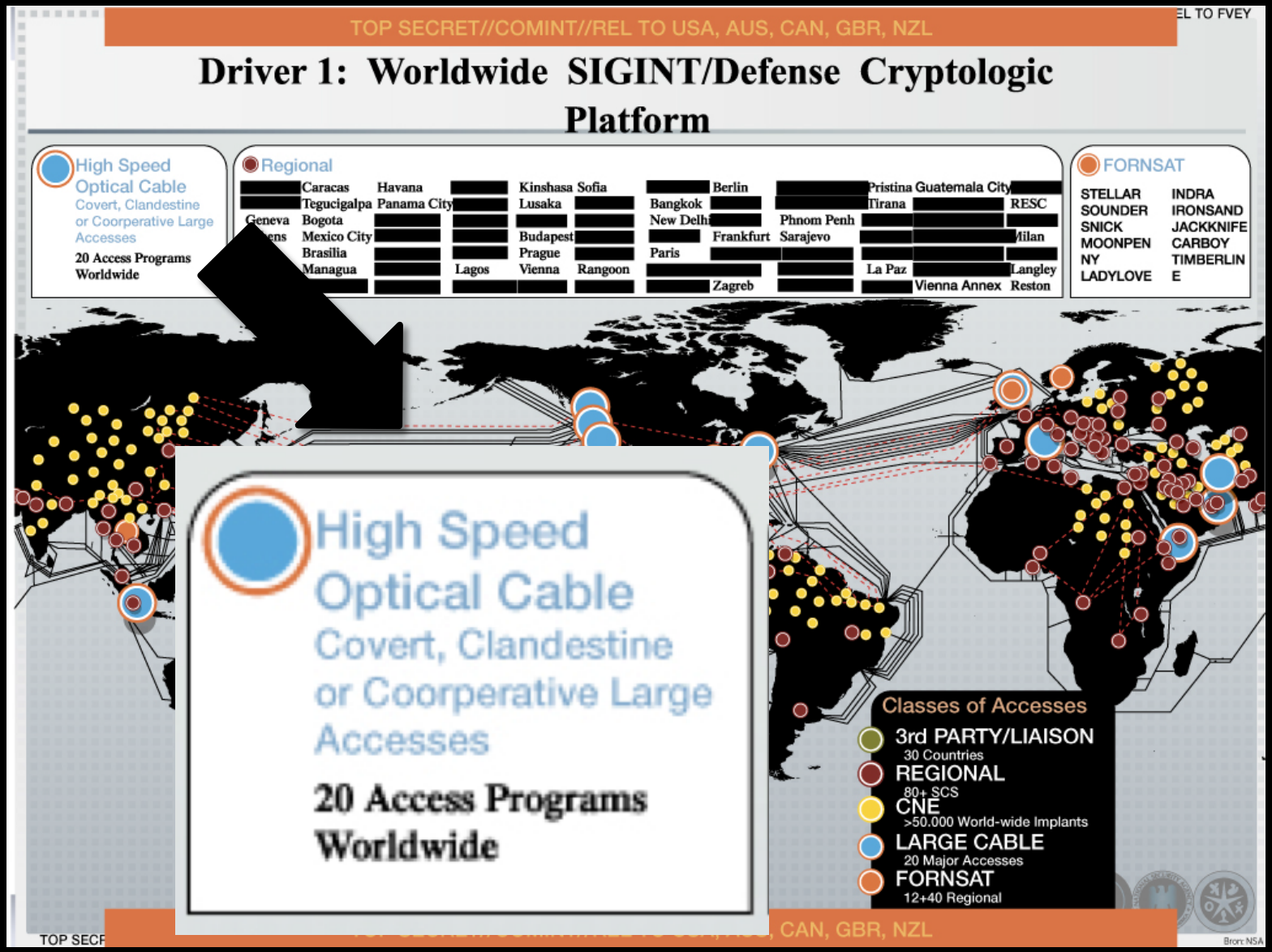
Source: Telegeography Research

TOP SECRET//SI//ORCON//NOFORN

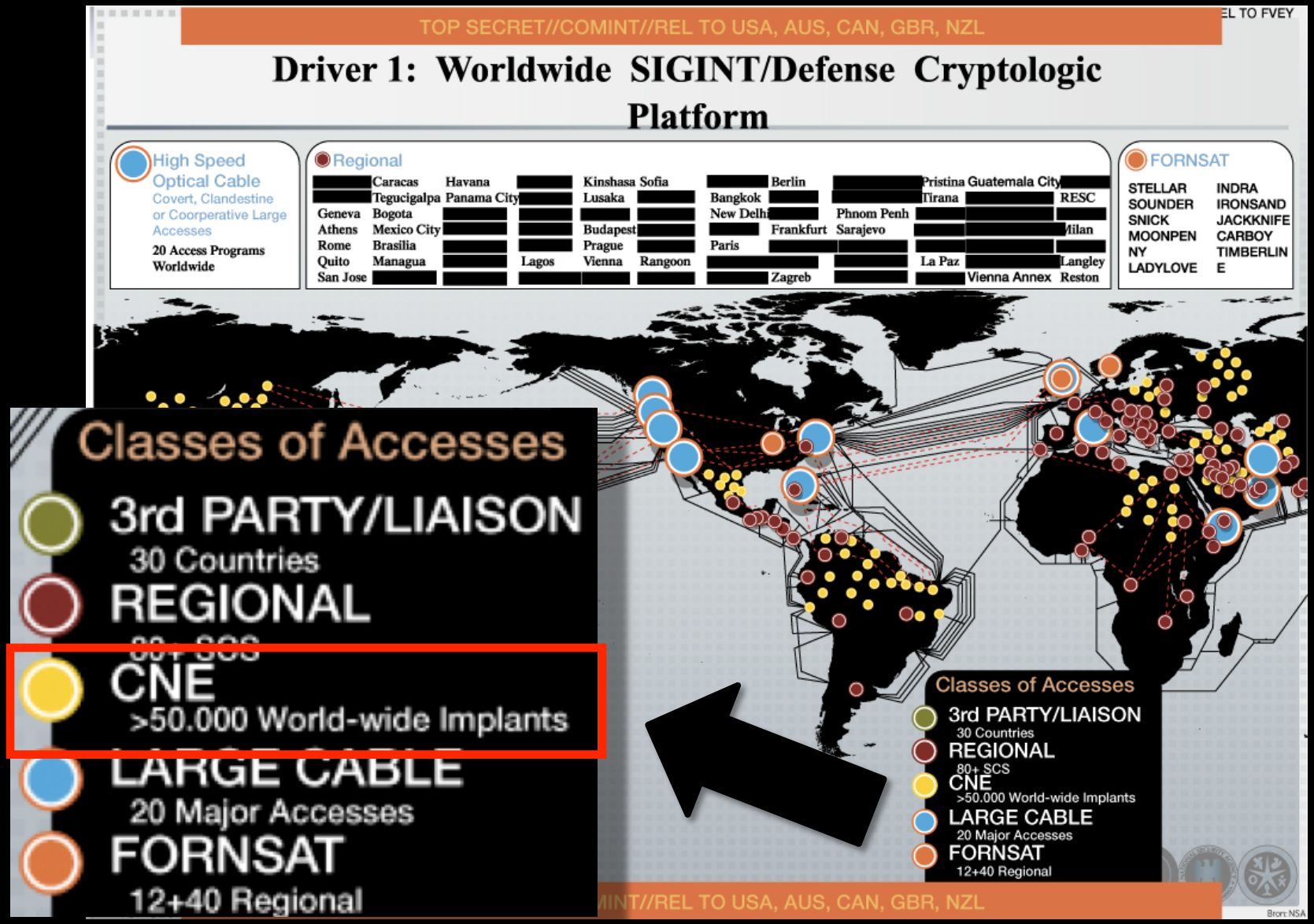
"Collect it all"



"Collect it all"

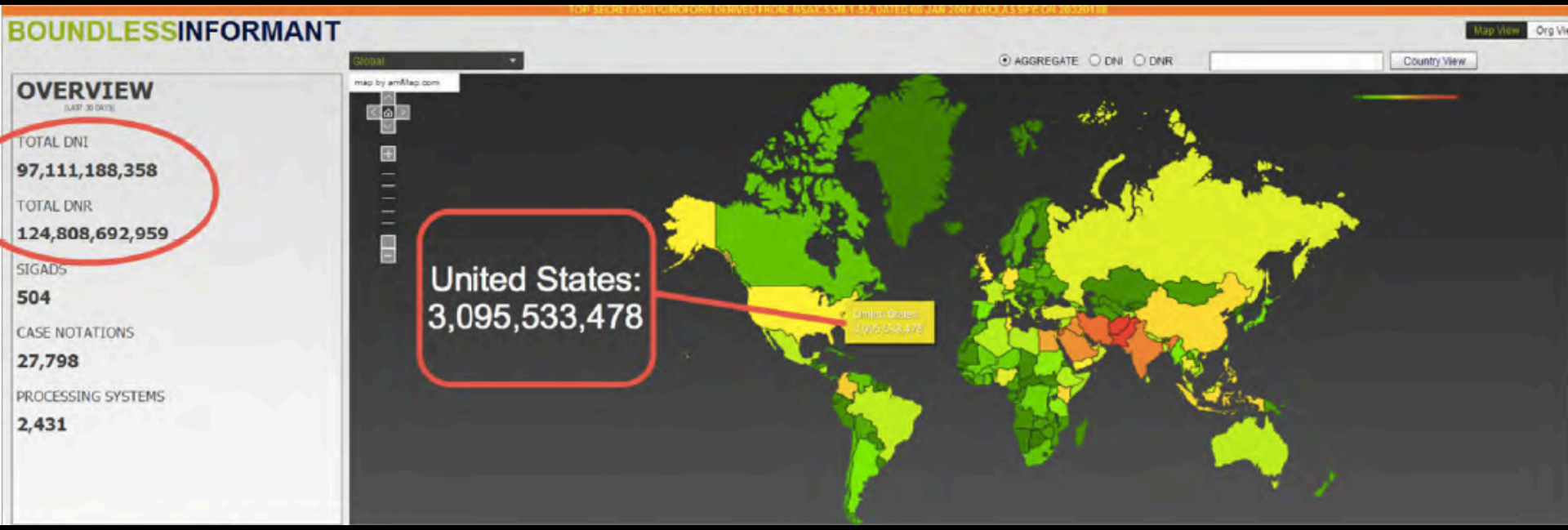


"Collect it all" + "Exploit it All"



Signal intelligence data caches

BOUNDLESS INFORMANT (Mar 2013)



- Denmark - 23 million telephone metadata records (in cooperation with the government)

The NSA is not operating alone

TOP SECRET// COMINT //REL USA, AUS, CAN, GBR, NZL

Approved SIGINT Partners

Second Parties

Australia
Canada
New Zealand
United Kingdom

Coalitions/Multi-lats

AFSC
NATO
SSEUR
SSPAC

Third Parties

Algeria
Austria
Belgium
Croatia
Czech Republic
Denmark
Ethiopia
Finland
France
Germany
Greece
Hungary
India
Israel
Italy
Japan
Jordan
Korea
Macedonia
Netherlands
Norway
Pakistan
Poland
Romania
Saudi Arabia
Singapore
Spain
Sweden
Taiwan
Thailand
Tunisia
Turkey
UAE

TOP SECRET// COMINT //REL USA, AUS, CAN, GBR, NZL

The NSA is not operating alone

TOP SECRET// COMINT //REL USA, AUS, CAN, GBR, NZL

Approved SIGINT Partners

Second Parties

Australia
Canada
New Zealand
United Kingdom

Coalitions/Multi-lats

AFSC
NATO
SSEUR
SSPAC

Third Parties

Algeria
Austria
Belgium
Croatia
Czech Republic
Denmark
Ethiopia
Finland
France
Germany
Greece
Hungary
India
Israel
Italy
Japan
Jordan
Norway
Pakistan
Poland
Romania
Saudi Arabia
Singapore
Spain
Sweden
Taiwan
Thailand

Denmark

TOP SECRET// COMINT //REL USA, AUS, CAN, GBR, NZL

Collection techniques

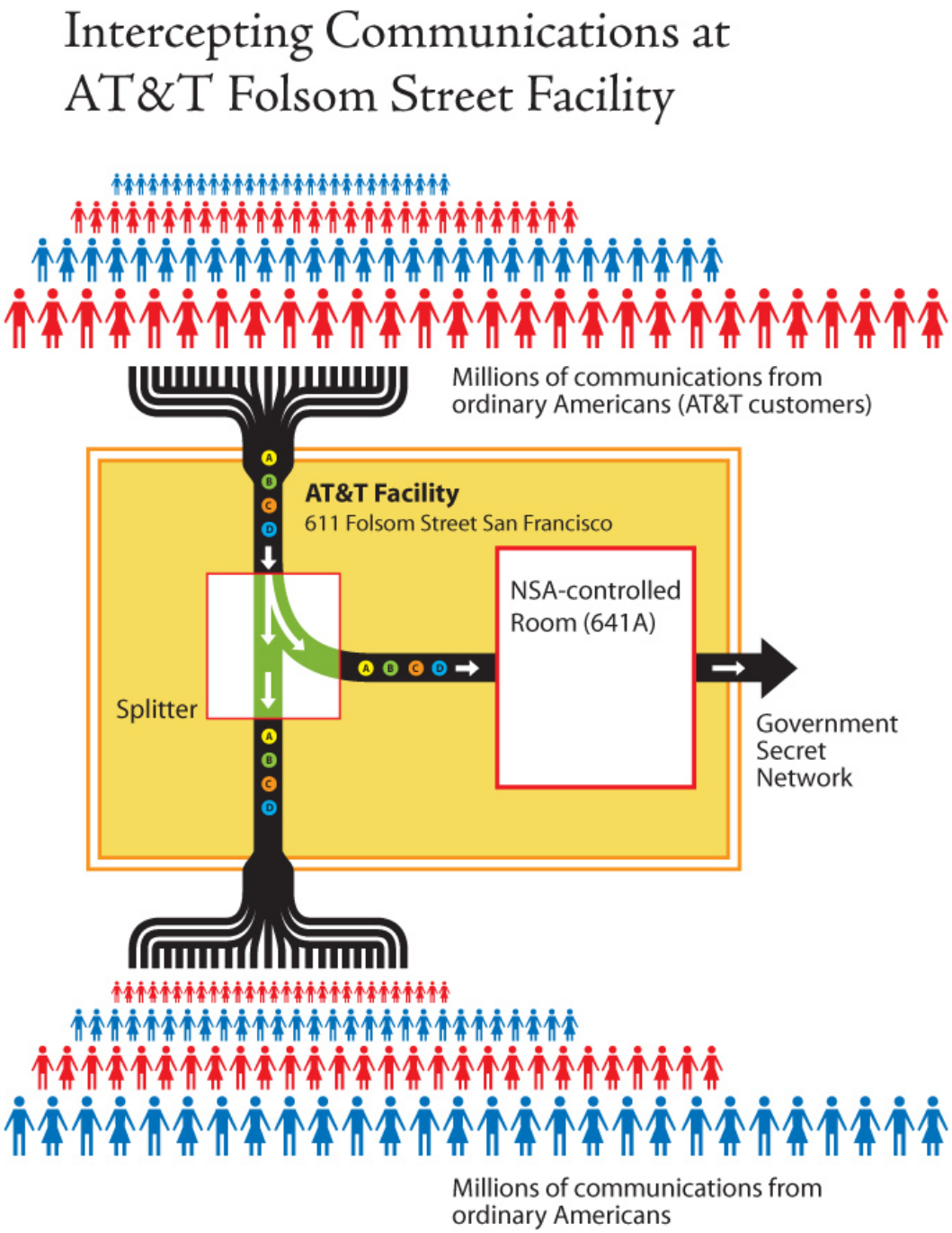
Upstream interception

AT&T SF regional switching centre

- 611 Folsom Street, San Francisco, site of known NSA warrantless 'Upstream' wiretapping (2006)

- 'Secret Room' 641a

EFF's view:



Source:
Electronic Frontier
Foundation (EFF)

IXmaps

see where your data packets go

Home | Tour | Explore | Contribute | Technical | FAQ | News & Events | About | Contact

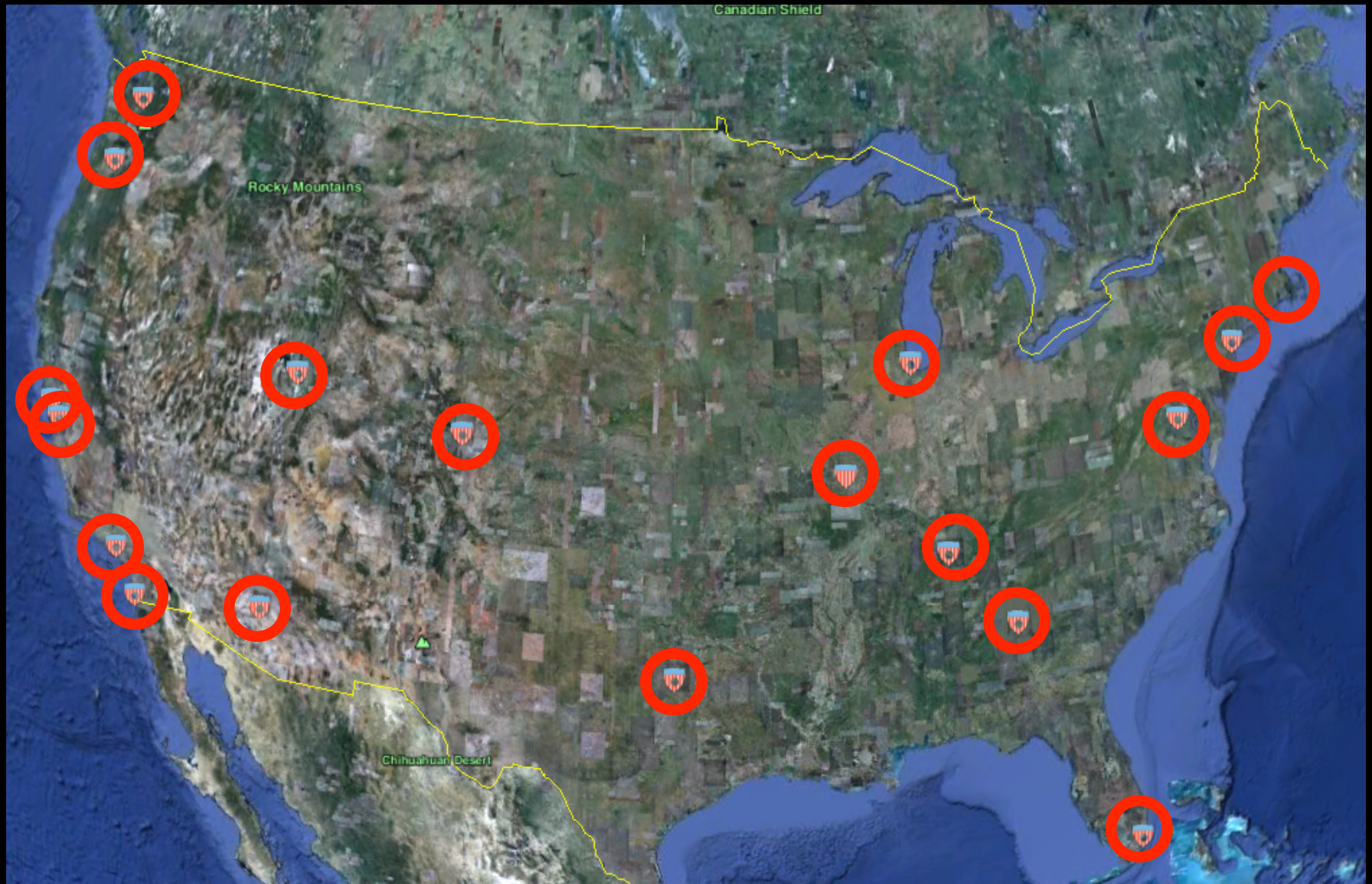
This beta version is being upgraded. We welcome your feedback

1 2 3 4

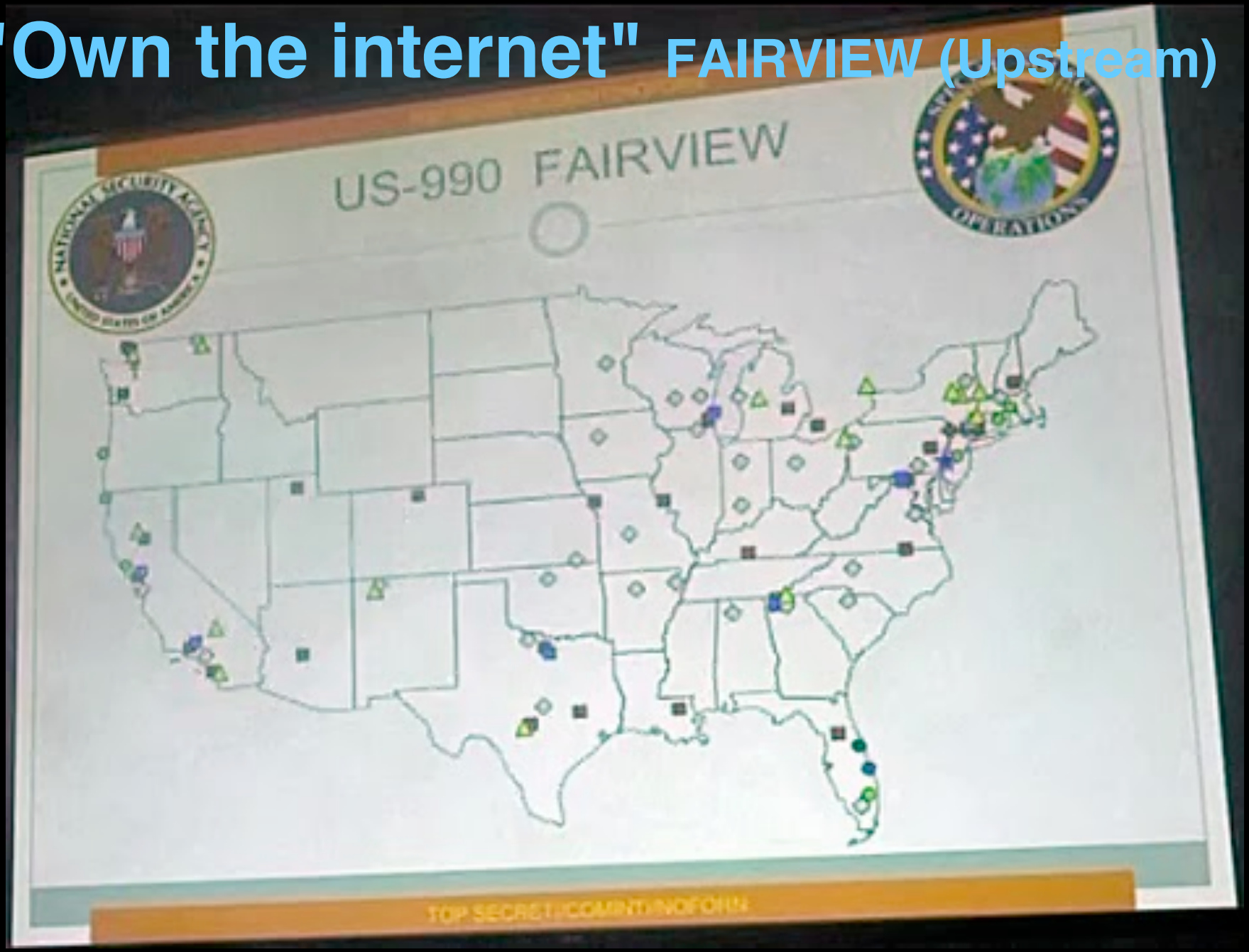
Who's looking at your data?

The U.S. National Security Agency (NSA) engages in warrantless internet surveillance. Mark Klein, a former AT&T technician turned whistleblower has revealed that the NSA has installed surveillance equipment at AT&T's main switching centre in San Francisco capable of intercepting all the data passing through it. The NSA is strongly suspected of operating similar spying facilities in 15-20 other U.S. cities. For example, one of our routes shows that data packets from Toronto to the San Francisco Art Institute pass through several such suspected sites. Learn more about who's looking at your data...

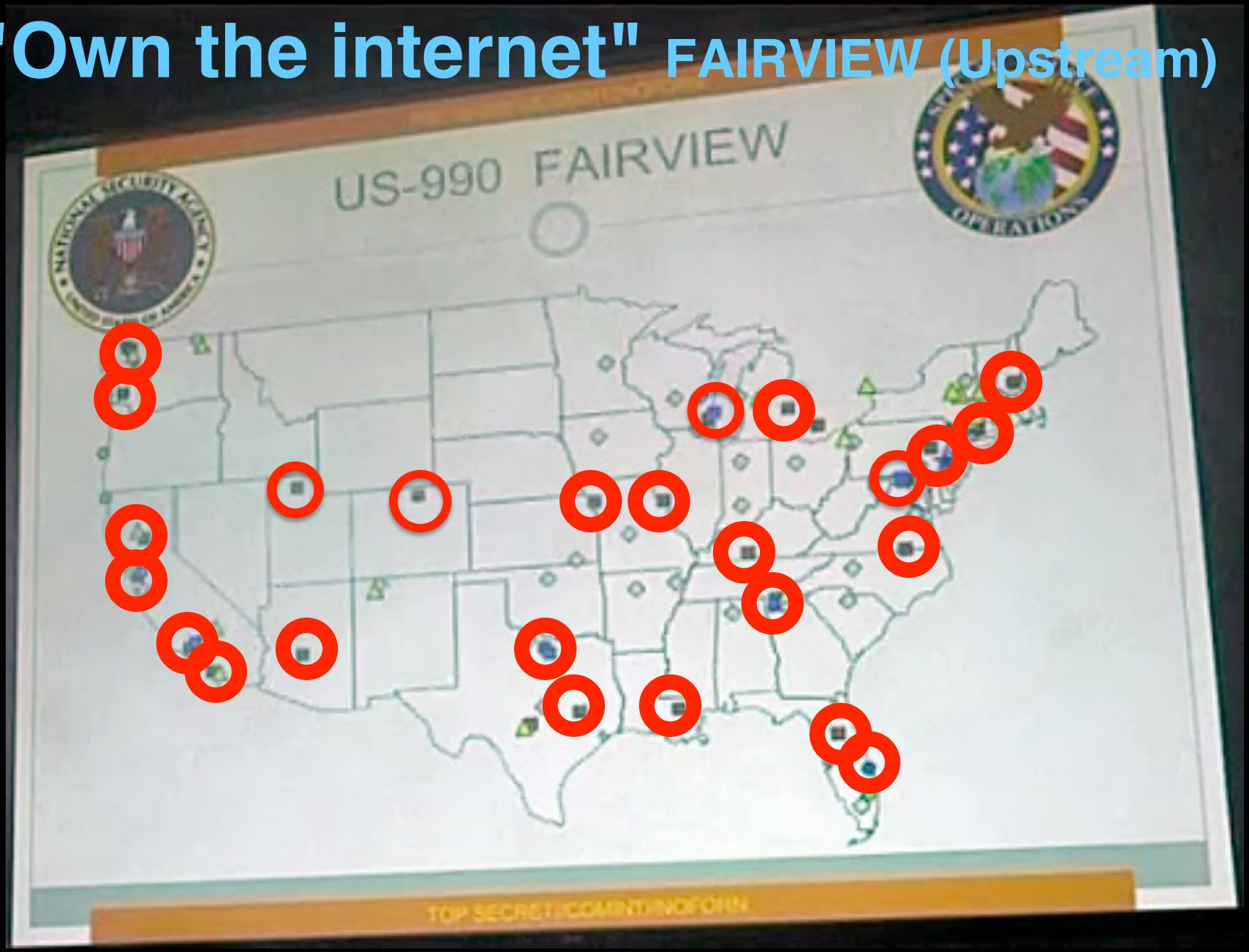
Suspected NSA splitter cities (2010)



"Own the internet" FAIRVIEW (Upstream)



"Own the internet" FAIRVIEW (Upstream)



Can US traffic avoid NSA cities?

Intra-US traceroutes	IXmaps DB	Percent
Total	1319	100%
Thru NSA cities	1312	99%
Bypass NSA cities	7	<1%

Counter-surveillance

Render this secret surveillance apparatus more transparent and accountable

IXmaps

see where your data packets go

Home | Tour | Explore | Contribute | Technical | FAQ | News & Events | About | Contact

This beta version is being upgraded. We welcome your feedback

1 2 3 4

Who's looking at your data?

The U.S. National Security Agency (NSA) engages in warrantless internet surveillance. Mark Klein, a former AT&T technician turned whistleblower has revealed that the NSA has installed surveillance equipment at AT&T's main switching centre in San Francisco capable of intercepting all the data passing through it. The NSA is strongly suspected of operating similar spying facilities in 15-20 other U.S. cities. For example, one of our routes shows that data packets from Toronto to the San Francisco Art Institute pass through several such suspected sites. Learn more about who's looking at your data...

IXmaps – Internet mapping platform

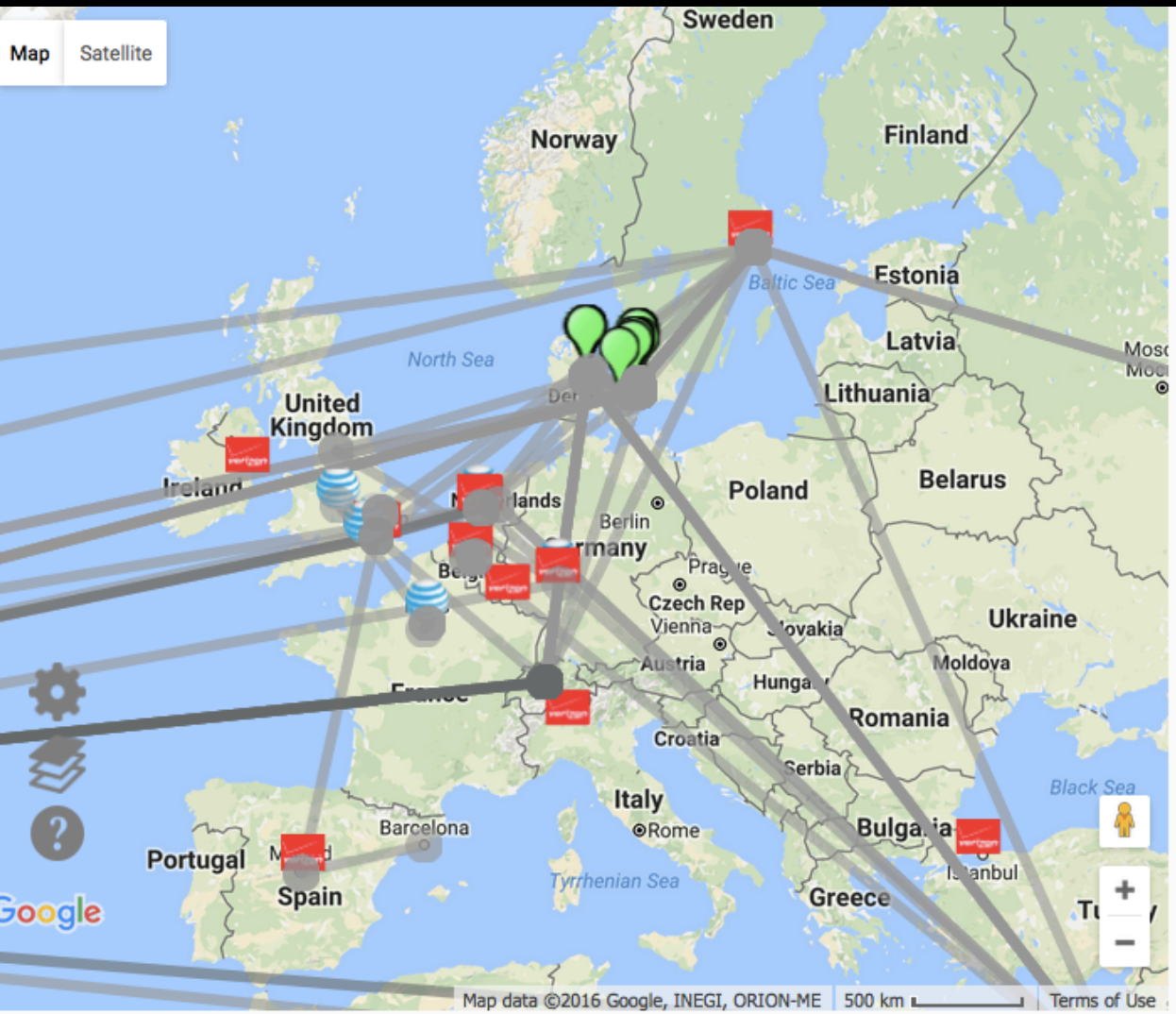
IXmaps

see where your data packets go

- Crowdsourced traceroute generation & collection
  > 150K TRs ~ 26K IP addresses
  > 600 contributors/origins ~ 4K destinations
- Systematic geo-location of individual data packet hops
- Map traceroute paths via GoogleMaps (> OpenStreetMap)
  – NSA surveillance, Google data centres, submarine cable overlays
- Custom filtering of traceroutes
  – NSA interception, 'boomerang routing,' ISP, city, ….
- Links hops/routers to ISPs + privacy transparency scores

Boomerang route:
Univ of Toronto > OSAP (Toronto)

Routes from Denmark



Traceroutes Found

Map All | Remove All

Displaying 42 of 42 sampled results (126 total)

ID	Origin	Dest. Hostname	Date
257960	DK	dr.dk	2016-04-01
232112	Greve, DK	facebook.com	2016-02-04
84692	Frederiksberg, DK	owncloud.itu.dk	2015-09-11
84684	Hørsholm, DK	netflix.com	2015-09-11
84678	Hørsholm, DK	salesforce.com	2015-09-11
84672	Hørsholm, DK	politiken.dk	2015-09-11
84666	Hørsholm, DK	tv2.dk	2015-09-11

Carrier Summary

Carrier	Rtrs.	Nat.	Transparency
TELIANET TeliaN...	41	EU	★
Danish network ...	37	DK	
ZENSYSTEMS-AS Z...	36	DK	
NORDUNET NORDUn...	30	SE	
GlobalConnect a...	15	DK	
COMCOR-AS AS fo...	13	JO	
Facebook, Inc.	11	NL	
CW Cable and Wi...	10	EU	

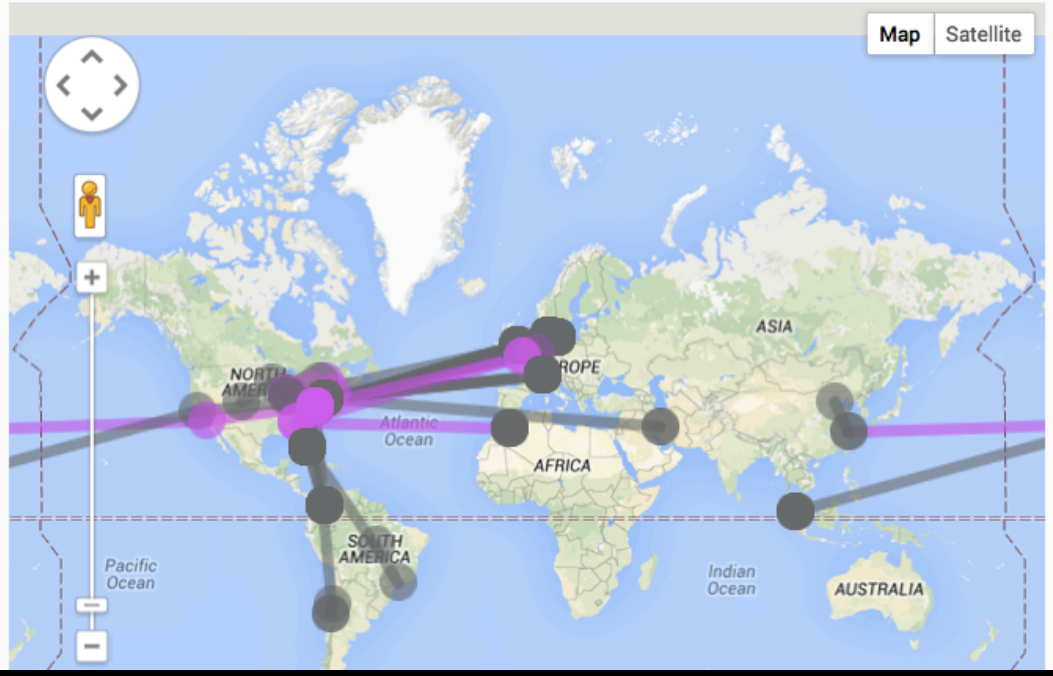
Routes from Denmark via US (and NSA) to 3rd countries

Custom Filters

Does	Originate in	Country	DK	AND
Does	Go Via	Country	US	AND
Does not	Terminate in	Country	US	AND

Total traceroutes : **12**

12 of 12 Add All Remove All



Asn	Carrier	Routers	Nat.	Score
174	Cogent	23	GB	(0)
2914	NTT/Verio	19	GB	
28717	ZENSYSTEMS-AS Zen Syst...	18	DK	
1299	TELIANET TeliaNet Glob...	15	EU	(0.5)
42525	GlobalConnect a/s Carr...	8	DK	
23520	Columbus Networks USA,...	6	US	
3603	University de Los Ande...	6	CO	
30983	MARWAN-AS	5	MA	
6939	Hurricane Electric, In...	5	NL	(2)
38182	Total Broadband Experi...	5	MY	

TRid: **69880**

View TR details

SNOWDEN SURVEILLANCE ARCHIVE

Archive | Portable Archive | Glossary | Help | Preferences | About

Open, indexed, searchable archive of published Snowden documents for journalist, academic, legal and lay research

Try it out! https://snowdenarchive.cjfe.org

SNOWDEN SURVEILLANCE ARCHIVE

Archive | Portable Archive | Glossary | Help | Preferences | About

Search for

	Words	... in field
	xkeyscore	All
and		Text
and		Description
and		Subject and Keywords

Word count: xkeyscore: 480

More than 50 documents matched the query.

XKEYSCORE Fingerprints

Document Source

Creating Agency:	**National Security Agency**
Date Created:	**ca.2012**
Classification:	**Unclassified / Unclassified**
Surveillance Program:	**XKEYSCORE**
Genre:	**Presentation slides : 1 p.**
Date Published:	**2014-06-16**
Journalist(s):	**Spiegel Staff**
Originating News Outlet:	**Der Spiegel**

Article Link

Web Forum Exploitation using XKEYSCORE

Document Source

Professional/political responses

Be skeptical of claims

- Ask questions, especially by promoters and secret agencies

Insist on transparency and accountability

- Discuss and develop official positions within professional associations (e.g. PROSA.dk – ????)
- Corporations, esp carriers/ISPs
  - eg Transparency reporting about gov access, routing, privacy protections
- Government agencies
  - Independent oversight bodies
- Work with Civil Liberties organizations

Technical/political responses

Obfuscation & Encryption (preferably end-to-end)

- Pretty Good Privacy (PGP/GPG) + …. See: Crypto Backers (Tuesday)
- Tor (the onion router)

Anonymity rights on-line (eg ICANN WhoIs proposal)

Keep cloud hosting local

- Avoid outsourcing to US corps, esp PRISM program providers

Avoid US (boomerang) routing

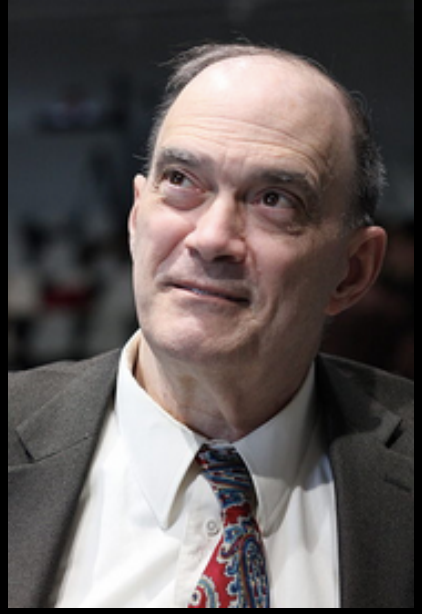
- Build internet capacity to keep domestic traffic local and route around US & Five Eyes partners

Level 3
Global Crossing
Verizon, Cogent, BT
++

"The disclosures that Edward Snowden revealed don't only expose a threat to our privacy but to our democracy itself."

Laura Poitras, 2015/2/22

Assistance needed



- Locate and map the sites of telecom interception worldwide
  - Fairview/ATT, Stormbrew/Verizon
  - + ???
- Work in progress with Bill Binney, ex-NSA official turned whistle blower
- Meet me after talk or email me:

  andrew.clement@utoronto.ca

CAUTION:

You become associated with me & Bill!

Readings

James Bamford

The Puzzle Palace: A Report on N.S.A., America's Most Secret Agency, 1982

Body of Secrets: Anatomy of the Ultra-Secret National Security Agency. (2002)

The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America. (2008)

Mark Klein*: Wiring up the Big Brother Machine* (2009)

Luke Harding: *The Snowden Files* (2014)

Glenn Greenwald: *No Place To Hide: Edward Snowden, the NSA, and the U.S. Surveillance State:* (2014)

See where your packets go!

(and contribute to the database) Feedback welcome

http://IXmaps.ca

These slides at : http://bit.ly/2diOAER

Project team:
Andrew Clement, Antonio Gamba, Colin McCann, Jonathan Obar & Dawn Walker
Faculty of Information, University of Toronto

Funding:
Social Sciences and Humanities Research Council (SSHRC)
Office of the Privacy Commissioner (OPC) of Canada
Canadian Internet Registration Authority (CIRA)