

# IXmaps or CHmaps

Rendering visible the  
'interesting' features of  
internet backbones,  
especially sites of  
surveillance



Andrew Clement, Steve Harvey, Nancy Paterson, David Phillips

Funded by SSHRC ITST grant

Affiliated with The New Transparency: Surveillance and Social Sorting,

SSHRC MCRI grant

<http://iprp.ischool.utoronto.ca/>

# Background

- Much is going on ‘inside’ the internet, but out of sight, that should concern users and policy advocates:
  - Surveillance (e.g eavesdropping by the NSA and other security agencies)
  - Deep packet inspection (DPI) by ISPs/carriers
  - Discriminatory traffic management and blockage
  - Excessive energy consumption
  - Oligopolistic and anti competitive business practices
  - ...
- There is relatively little critical research into, or public understanding of, internet backbone structure and operation
- Prevailing metaphors, such as ‘dumb core/ intelligent edges’ and ‘cloud computing’, obscure important insights and possibilities for action

# Research ambitions

- Make visible to users interesting internet backbone/core phenomena related to everyday usage
  - e.g. NSA surveillance, DPI, Carrier Hotel ownership, energy (in)efficiency, ...
- Promote an understanding of the internet core amenable to public policy engagement
- Develop a research tool for conducting critical internet backbone investigations, and for presenting findings publically
- Enroll others (users, activists, researchers) in building the database of internet sites of interest

# Welcome screen (mock up)

## Welcome to IXmaps

This tool allows you to trace the route your packets take across the internet when you visit a web site

Please enter a destination URL \_\_\_\_\_  
or select a start and destination node  
from the map on the right.

Please select the types of site along the  
route you are interested in learning  
about:

- NSA eavesdropping
- ISPs
- DPI routers
- Energy efficiency
- ...



# Welcome screen (mock up)

## Welcome to IXmaps

This tool allows you to trace the route your packets take across the internet when you visit a web site

Please enter a destination URL \_\_\_\_\_  
or select a start and destination node  
from the map on the right.

Please select the types of site along the  
route you are interested in learning  
about:

- NSA eavesdropping
- ISPs
- DPI routers
- Energy efficiency
- ...



# Summary screen

From: [utoronto.ca](http://utoronto.ca) To: [ucsd.edu](http://ucsd.edu)

6 internet exchange points

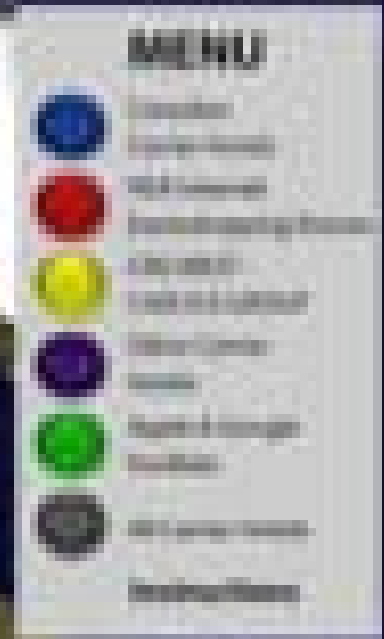
• NSA eavesdropping sites: 2

• DPI using ISPs: 3

• Carlyle group carrier hotels: 2

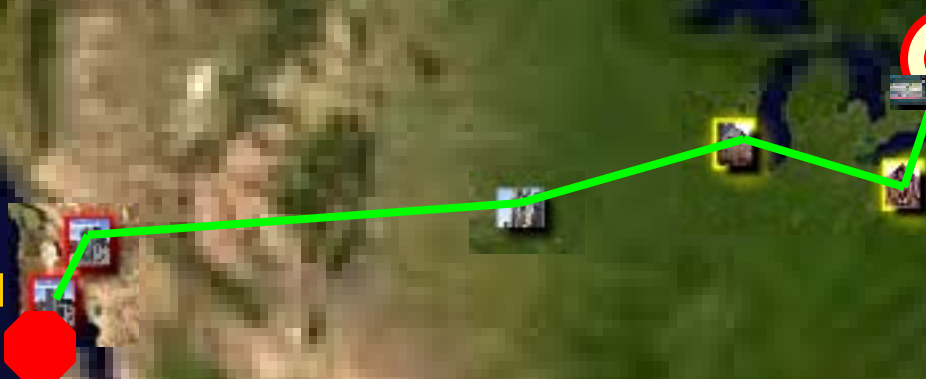
• Other carrier hotels: 2

Click on images to see further details



[ucsd.edu](http://ucsd.edu)

[utoronto.ca](http://utoronto.ca)



# Summary screen (Google Earth)

The screenshot shows the Google Earth interface with a network diagram connecting Toronto (utoronto.ca) and San Diego (ucsd.edu). A yellow-bordered box in the center of the map contains the following text:

**From: utoronto.ca To: ucsd.edu**  
**6 Internet Exchange Points**  
**NSA eavesdropping sites: 2**  
**Carlyle group carrier hotels: 3**  
**Other carrier hotels: 1**  
**Click on images to see further details**

The network diagram includes nodes for ucsd.edu, ATT 611 Folsom, Omaha, NB, Cincinnati, 427 South LaSalle, Chicago, and utoronto.ca. The interface also shows the Search, Places, and Layers panels on the left side.

**Search**  
Fly To Find Businesses Directions  
Fly to e.g., 37.25.818' N, 122.05.36' W  
[Search Box]

**Places** Add Content  
CHMaps  
Instructions  
5 hops  
ucsd.edu  
name/ip/ms: ucsd.edu / 132.239.180.101 AS7377 /  
ATT 611 Folsom

**Layers**  
Primary Database  
Geographic Web  
Roads  
3D Buildings  
Street View  
Borders and Labels  
Traffic  
Weather

2009 Europa Technologies  
© 2009 Tele Atlas  
Data SIO, NOAA, U.S. Navy, NGA, GEBCO  
© 2009 Google  
lat 44.468570° lon -105.846224° elev 1107 m  
Eye at 4430.27 km





# TR details screen

| Hop# | IP#             | Delay | Lat    | Long    | AS#   | DPI# | CH# | ISP     | NSA |
|------|-----------------|-------|--------|---------|-------|------|-----|---------|-----|
| 1    | 192.168.1.1     |       |        |         |       |      |     |         |     |
| 2    | 206.248.154     | 10    | 42.4   | -82.183 | 12345 |      |     | TekSav  |     |
| 3    | 69.196.136.     | 8     | 43.667 | -79.417 | 12345 |      | 151 | TekSav  |     |
| 4    | 65.39.198.2     | 8     | 43.667 | -79.417 | 24680 | 198  | 151 | Peer 1  |     |
| 5    | 216.187.114     | 69    | 40.689 | -74.02  | 24680 | 198  | 232 | Peer 1  | 11  |
| 6    | 216.187.88.     | 73    | 40.689 | -74.02  | 24680 | 198  | 232 | Peer 1  | 11  |
| 7    | 216.187.88.     | 91    | 40.689 | -74.02  | 24680 | 198  | 232 | Peer 1  | 11  |
| 8    | 198.32.176.     | 82    | 33.978 | -118.44 | 43210 |      | 323 | EP.NET, |     |
| 9    | 137.164.47.     | 84    | 33.819 | -118.04 | 76859 |      |     |         |     |
| 10   | 137.164.46.     | 85    | 33.819 | -118.04 | 76859 |      |     |         |     |
| 11   | 137.164.46.     | 97    | 33.819 | -118.04 | 76859 |      |     |         |     |
| 12   | 137.164.47.     | 98    | 33.819 | -118.04 | 76859 |      |     |         |     |
| 13   | 137.164.24.     | 98    | 33.819 | -118.04 | 76859 |      |     |         |     |
| 14   | 132.239.255     | 98    | 32.881 | -117.24 | 97531 |      |     |         |     |
| 15   | 132.239.254     | 98    | 32.881 | -117.24 | 97531 |      |     |         |     |
|      | 132.239.180.101 |       |        |         |       |      |     |         |     |

Carrier hotel -  
151 Front St.  
Toronto



# TR details screen

| Hop# | IP#             | Delay | Lat    | Long    | AS#   | DPI# | CH# | ISP    | NSA |
|------|-----------------|-------|--------|---------|-------|------|-----|--------|-----|
| 1    | 192.168.1.1     |       |        |         |       |      |     |        |     |
| 2    | 206.248.154     | 10    | 42.4   | -82.183 | 12345 |      |     | TekSav |     |
| 3    | 69.196.136.     | 8     | 43.667 | -79.417 | 12345 |      | 151 | TekSav |     |
| 4    | 65.39.198.2     | 8     | 43.667 | -79.417 | 24680 | 198  | 151 | Peer 1 |     |
| 5    | 216.187.114     | 69    | 40.689 | -74.02  | 24680 | 198  | 232 | Peer 1 | 11  |
| 6    | 216.187.88.     | 73    | 40.689 | -74.02  | 24680 | 198  | 232 | Peer 1 | 11  |
| 7    | 216.187.88.     | 91    | 40.689 | -74.02  | 24680 | 198  | 232 | Peer 1 | 11  |
| 8    | 198.32.176.     | 82    | 33.978 | -118.44 | 43210 |      | 323 | EP.NET |     |
| 9    | 137.164.47.     | 84    | 33.819 | -118.04 | 76859 | 357  | 444 | CENIC  | 22  |
| 10   | 137.164.46.     | 85    | 33.819 | -118.04 | 76859 | 357  | 444 | CENIC  | 22  |
| 11   | 137.164.46.     | 97    | 33.819 | -118.04 | 76859 | 357  | 444 | CENIC  | 22  |
| 12   | 137.164.47.     | 98    | 33.819 | -118.04 | 76859 | 357  | 444 | CENIC  | 22  |
| 13   | 137.164.24.     | 98    | 33.819 | -118.04 | 76859 | 357  | 444 | CENIC  | 22  |
| 14   | 132.239.255     | 98    | 32.881 | -117.24 | 97531 |      |     | UCSD   |     |
| 15   | 132.239.254     | 98    | 32.881 | -117.24 | 97531 |      |     | UCSD   |     |
|      | 132.239.180.101 |       |        |         |       |      |     |        |     |

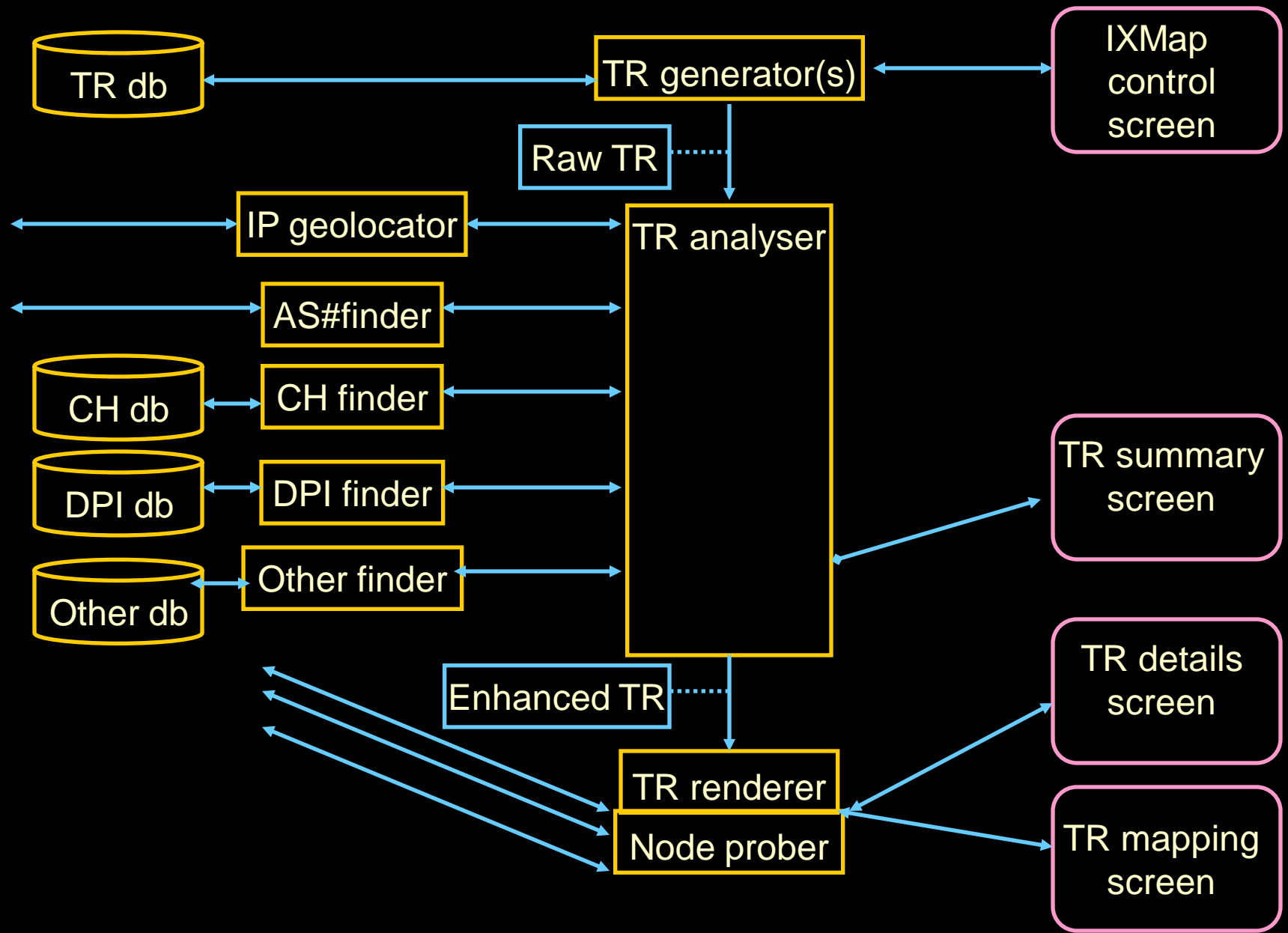
NSA  
warrantless  
wiretapping  
sites  
(suspected  
– see  
Marcus  
deposition,  
2006)

# TR details screen

| Hop# | IP#             | Delay | Lat    | Long    | AS#   | DPI# | CH# | ISP     | NSA |
|------|-----------------|-------|--------|---------|-------|------|-----|---------|-----|
| 1    | 192.168.1.1     |       |        |         |       |      |     |         |     |
| 2    | 206.248.154     | 10    | 42.4   | -82.183 | 12345 |      |     | TekSav  |     |
| 3    | 69.196.136.     | 8     | 43.667 | -79.417 | 12345 |      | 151 | TekSav  |     |
| 4    | 65.39.198.2     | 8     | 43.667 | -79.417 | 24680 | 198  | 151 | Peer 1  |     |
| 5    | 216.187.114     | 69    | 40.689 | -74.02  | 24680 | 198  | 232 | Peer 1  | 11  |
| 6    | 216.187.88.     | 73    | 40.689 | -74.02  | 24680 | 198  | 232 | Peer 1  | 11  |
| 7    | 216.187.88.     | 91    | 40.689 | -74.02  | 24680 | 198  | 232 | Peer 1  | 11  |
| 8    | 198.32.176.     | 82    | 33.978 | -118.44 | 43210 |      | 323 | EP.NET, |     |
| 9    | 137.164.47.     | 84    | 33.819 | -118.04 | 76859 | 357  | 444 | CENIC   | 22  |
| 10   | 137.164.46.     | 85    | 33.819 | -118.04 | 76859 | 357  | 444 | CENIC   | 22  |
| 11   | 137.164.46.     | 97    | 33.819 | -118.04 | 76859 | 357  | 444 | CENIC   | 22  |
| 12   | 137.164.47.     | 98    | 33.819 | -118.04 | 76859 | 357  | 444 | CENIC   | 22  |
| 13   | 137.164.24.     | 98    | 33.819 | -118.04 | 76859 | 357  | 444 | CENIC   | 22  |
| 14   | 132.239.255     | 98    | 32.881 | -117.24 | 97531 |      |     | UCSD    |     |
| 15   | 132.239.254     | 98    | 32.881 | -117.24 | 97531 |      |     | UCSD    |     |
|      | 132.239.180.101 |       |        |         |       |      |     |         |     |

Peer 1  
Networks  
operates  
Narus 1234  
Semantic  
Traffic  
Analyzer, for  
unknown  
purposes

# System side IXMap system overview User side



# Future work

- Working prototype as proof of concept
- Build data base of:
  - Trace routes
  - NSA sites
  - DPI sites and policies
  - Energy consumers
- Art gallery installation?
- Cyber-surveillance international research workshop, May 2011, Toronto
- > Looking for research assistant(s)