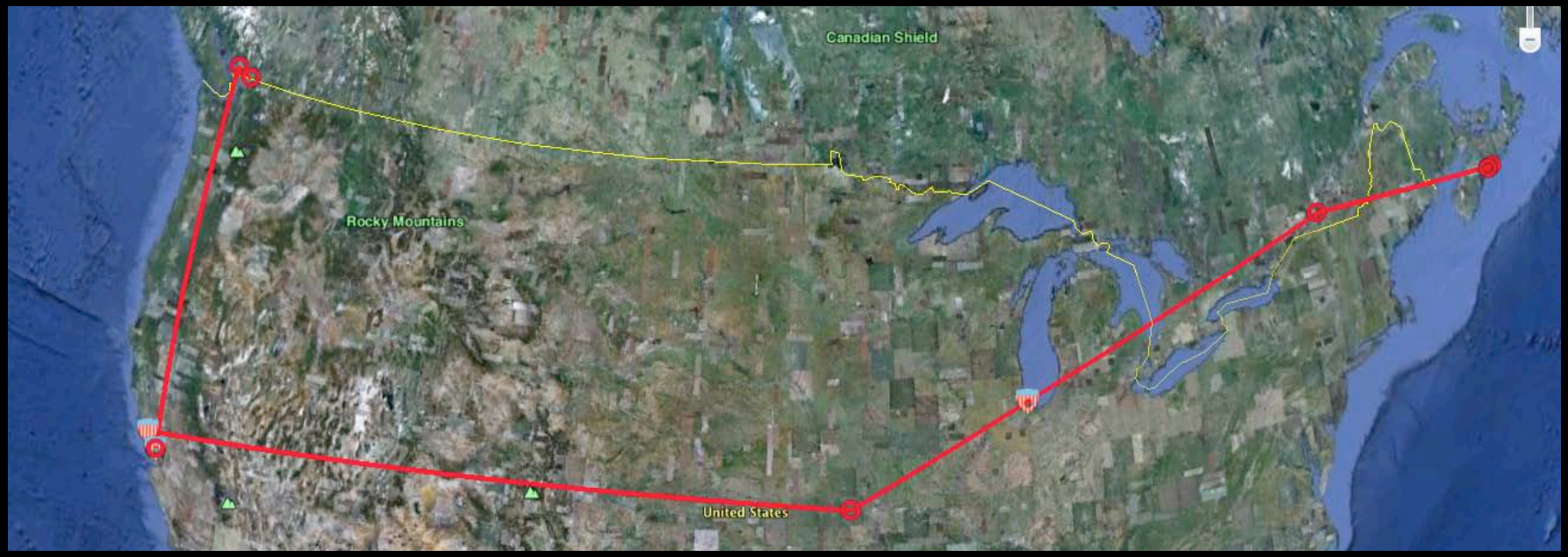
"Boomerang" routing

Visualizing Canada/US cross-border traffic and surveillance



Andrew Clement

with Steve Harvey, Yannet Lathrop, Colin McCann, Nancy Paterson,** David Phillips, Gabby Resch & Erik Stewart

Faculty of Information, U of T; ** also with OCADU

The New Transparency: Surveillance and Social Sorting

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

CloudLaw Conference

Law and Policy in the Cloud

Centre for Innovation Law & Policy

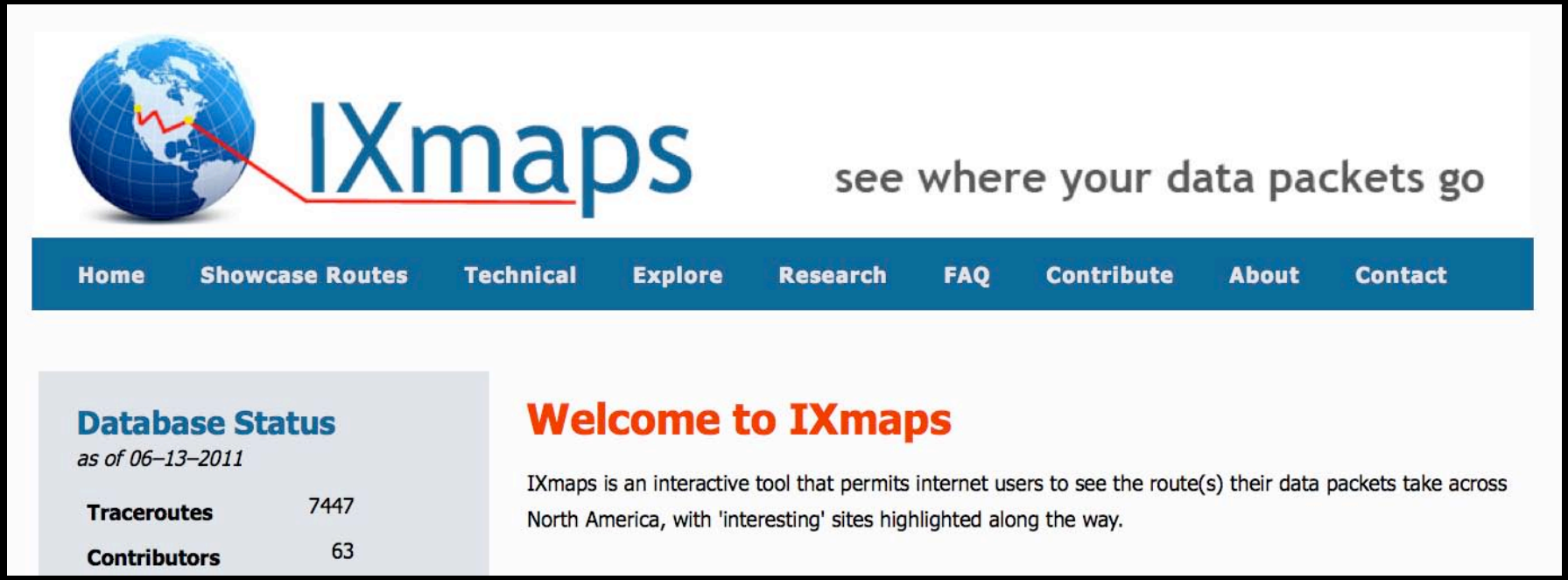
University of Toronto

Oct 14, 2011

Motivation

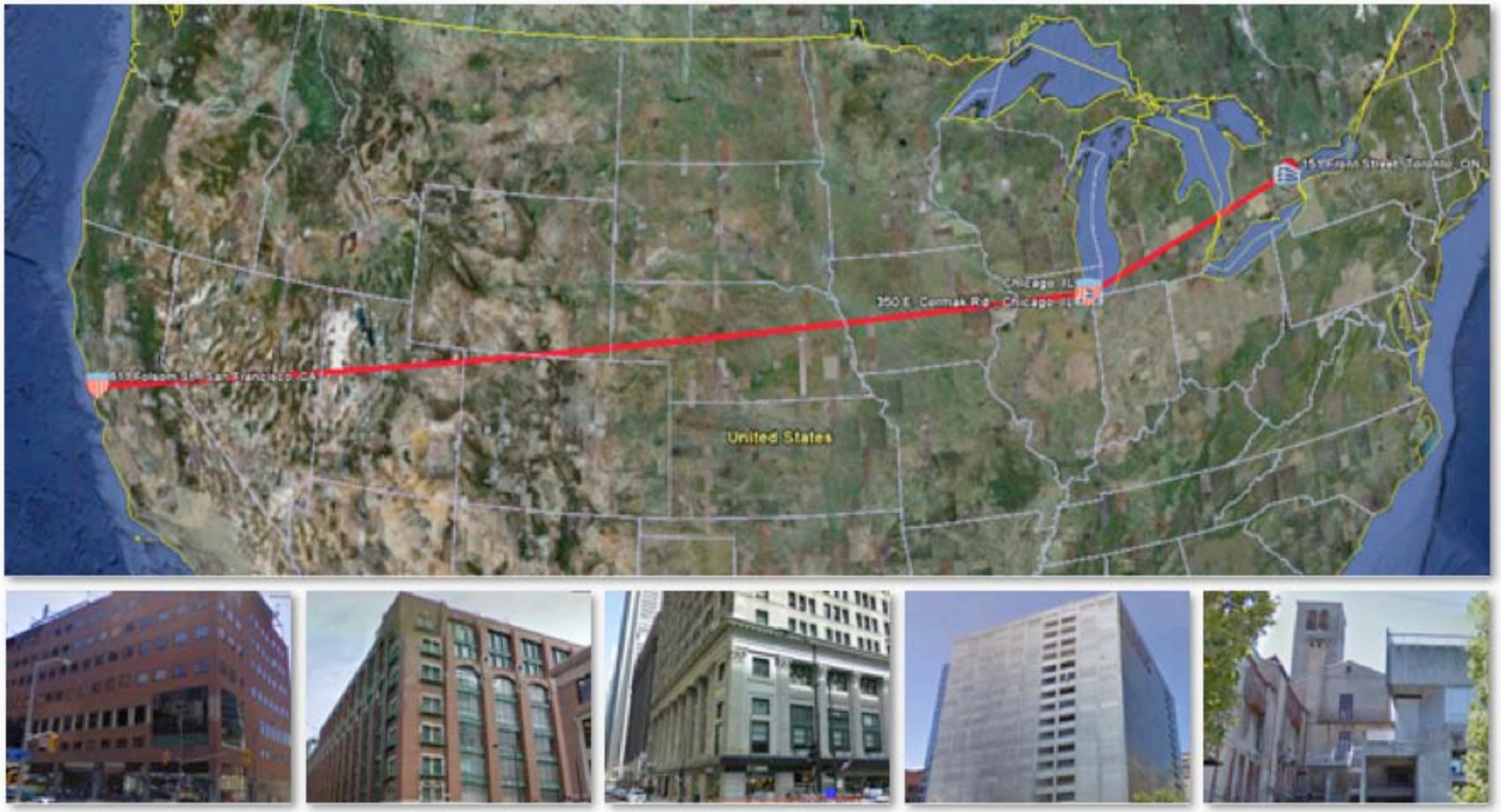
- Much is going on ‘inside’ the internet, but out of sight, that should concern users and public interest policy advocates:
  - Surveillance (e.g. eavesdropping by the NSA and other security agencies)
  - Deep packet inspection (DPI) by ISPs/carriers
  - Discriminatory traffic management and blockage
  - Oligopolistic and anti-competitive business practices
  - …
- ‘Cloud computing’ as a metaphor obscures important insights and possibilities for action

IXmaps.ca – visualizing internet routing

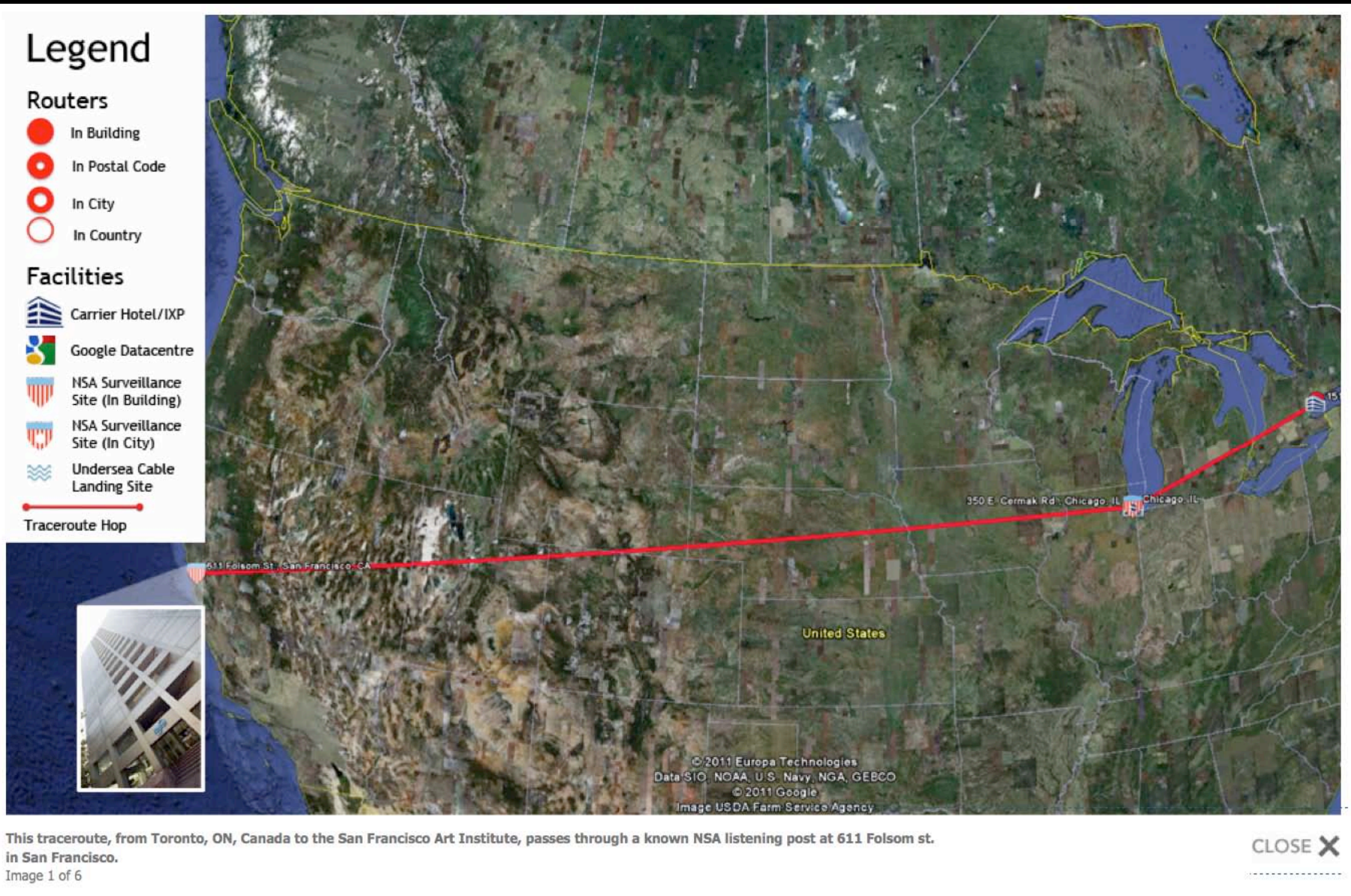


- Crowd-sourced traceroute generation across North America
- Google Earth mash-up
  - Traceroutes, internet exchange points (IXPs), carrier hotels, “interesting” site info

The Internet is not a cloud!



Toronto > San Francisco (TR1859)

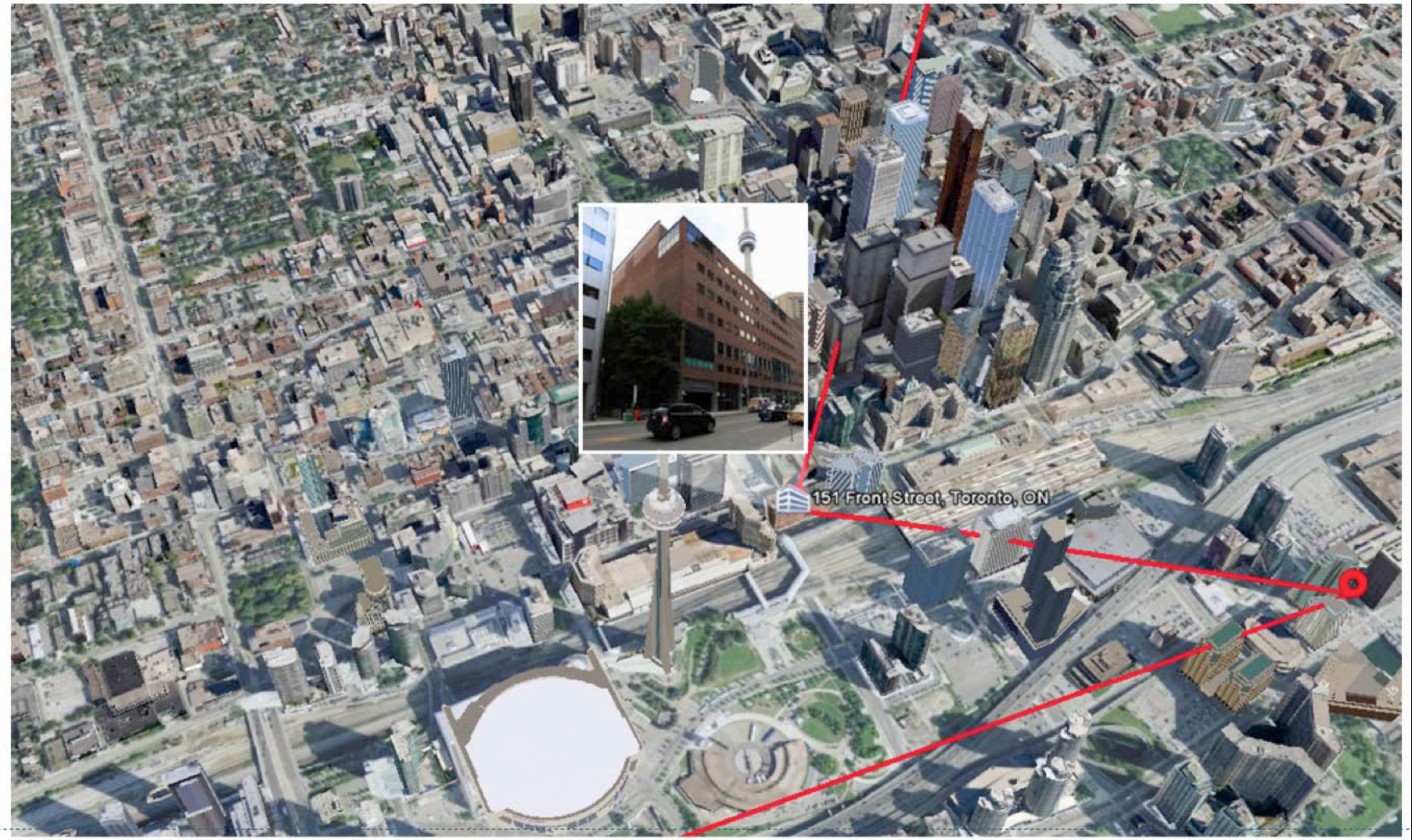


This traceroute, from Toronto, ON, Canada to the San Francisco Art Institute, passes through a known NSA listening post at 611 Folsom st. in San Francisco.

Image 1 of 6

CLOSE

Toronto: 151 Front Street

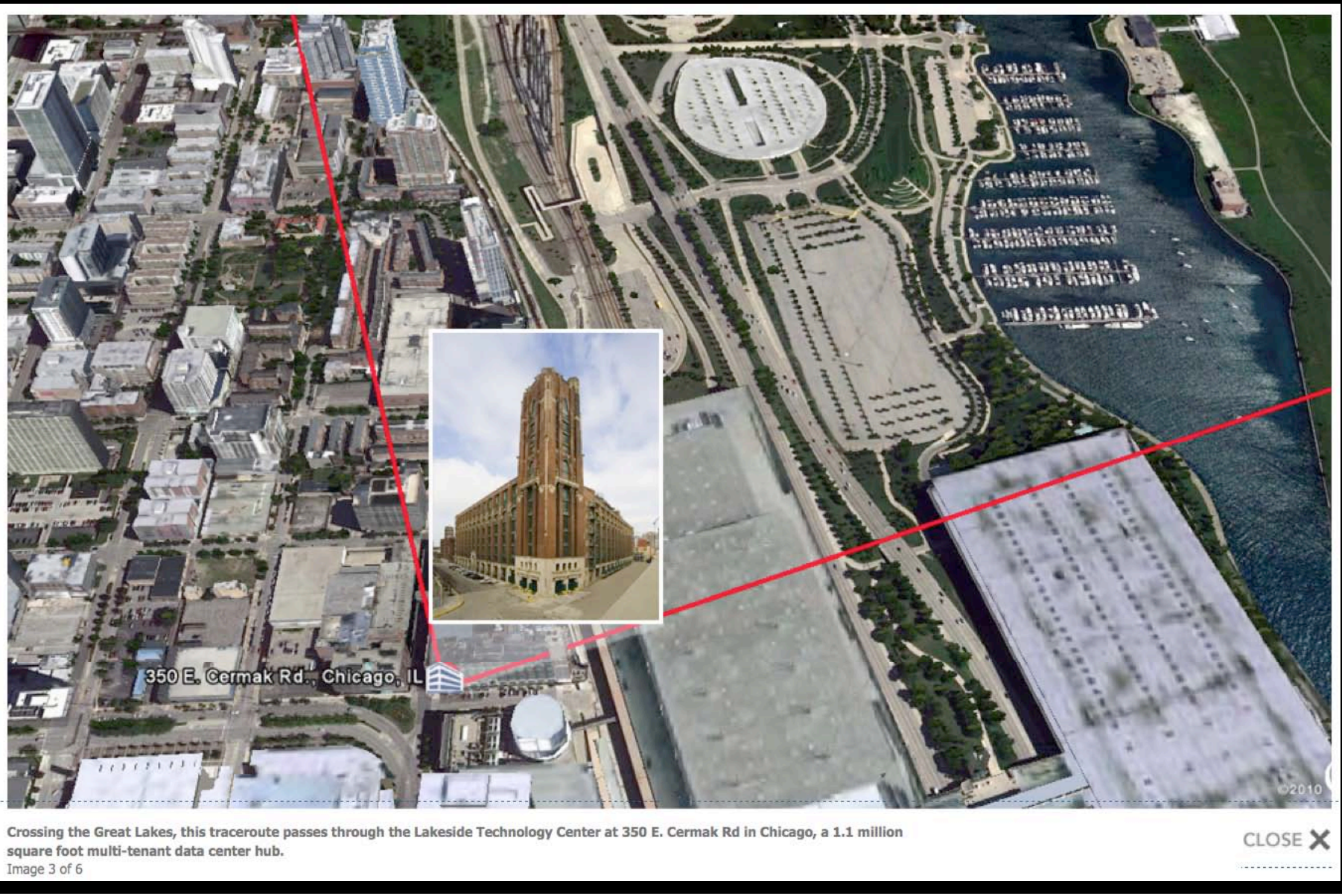


Originating in Toronto, this traceroute passes through 151 Front Street, a major carrier hotel that houses over 100 telecommunications companies, and is Canada's premier telecommunications hub.

Image 2 of 6

CLOSE ✕

Chicago: 350E Cermak Rd.

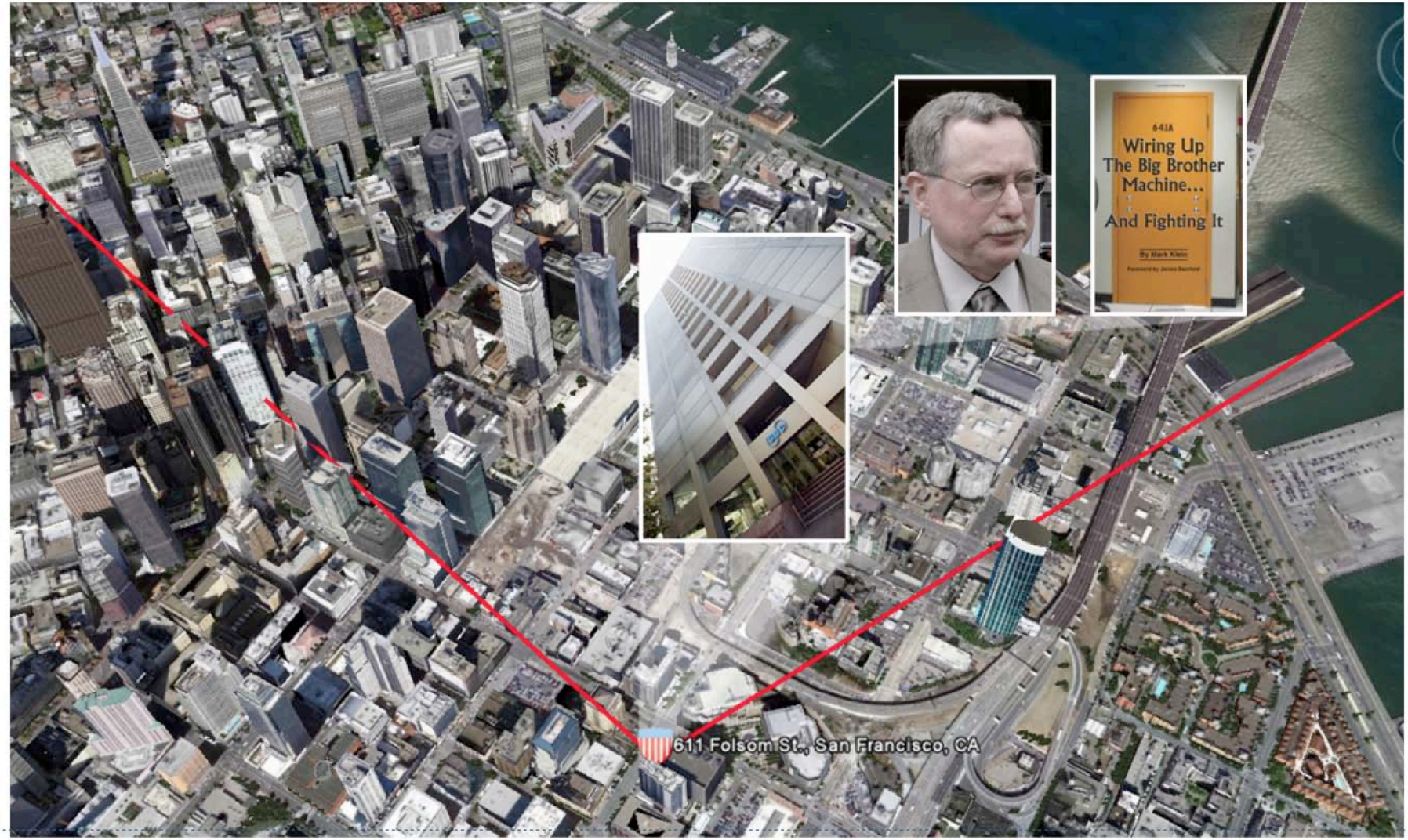


Crossing the Great Lakes, this traceroute passes through the Lakeside Technology Center at 350 E. Cermak Rd in Chicago, a 1.1 million square foot multi-tenant data center hub.

Image 3 of 6

CLOSE ✕

San Francisco: 611 Folsom Street



Near the end of its path, this traceroute passes through 611 Folsom Street, in San Francisco, a known NSA listening post. The existence of room 641A, an intercept facility operated by AT&T for the NSA, was documented by former network engineer and whistleblower, Mark Klein.

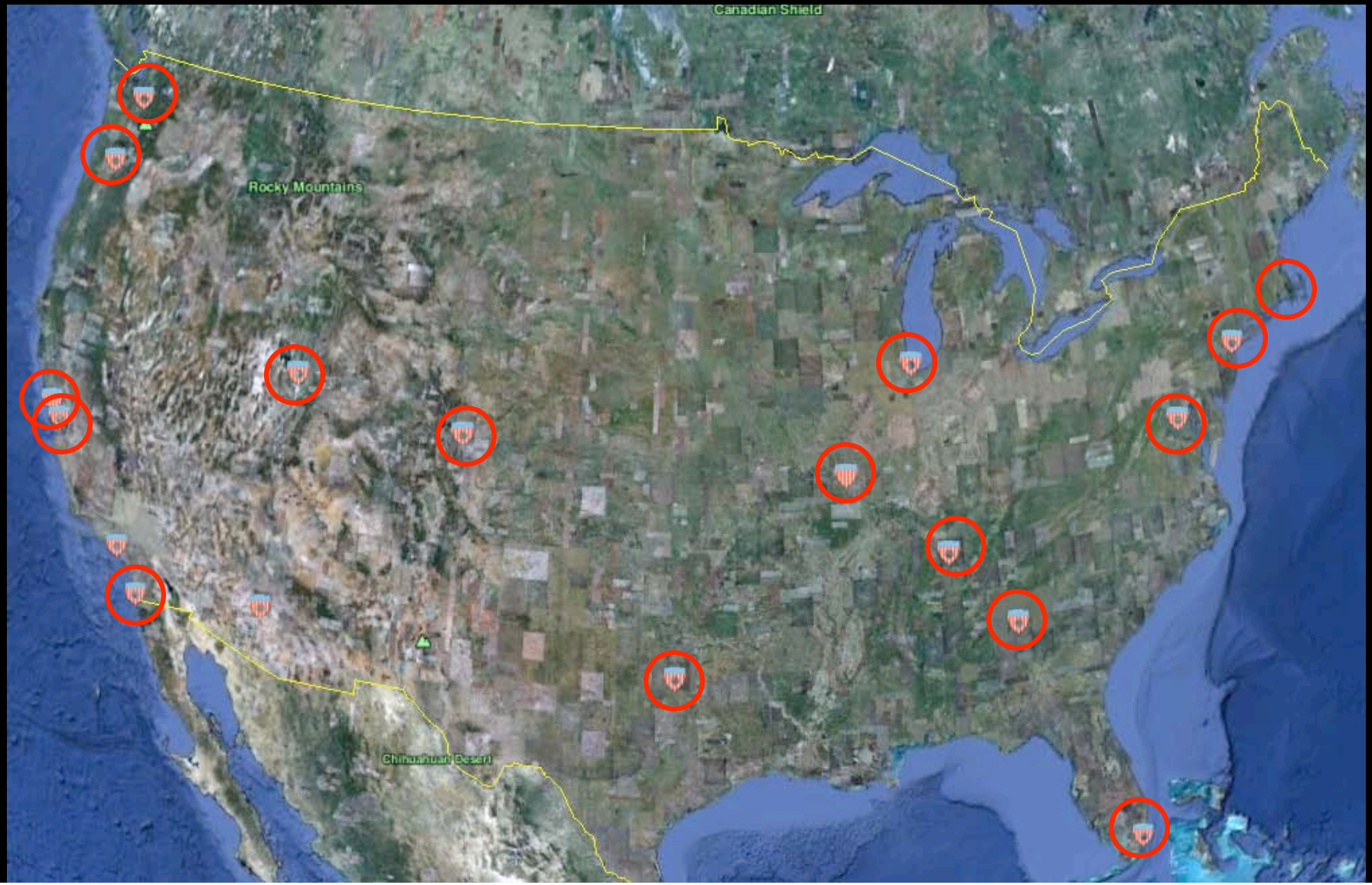
Image 5 of 6

CLOSE ✕

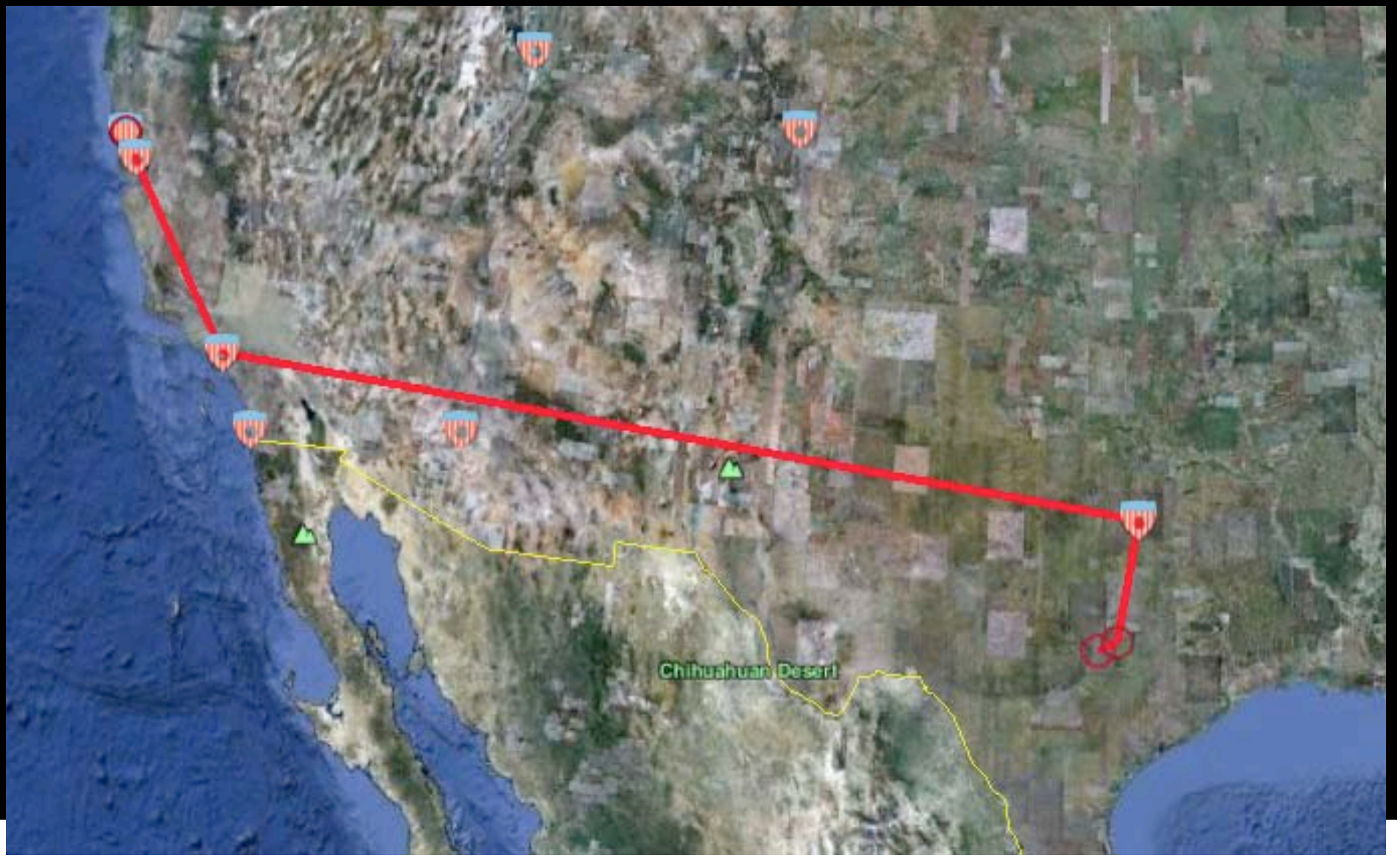
Internet surveillance

- USA PATRIOT Act
  - Expanded surveillance capabilities
    - Interception of messages
  - Extends to “protected computers” outside the US
  - Gag orders
- NSA Warrantless Wiretapping
  - Fibre-optic “splitters” at major internet gateways
    - San Francisco, Seattle, San Jose, Los Angeles, San Diego, Atlanta, + ~10 others (see Klein 2009; Bamford, 2008)
  - Traffic screened at carrier speed (10Gb/sec) and selectively stored by NSA (see Landau, 2011)

Suspected NSA surveillance sites



Austin TX > San Francisco Law Library, SF CA (TR1751)



Austin TX > San Francisco Law Library, SF CA (TR1751)

Traceroute detail

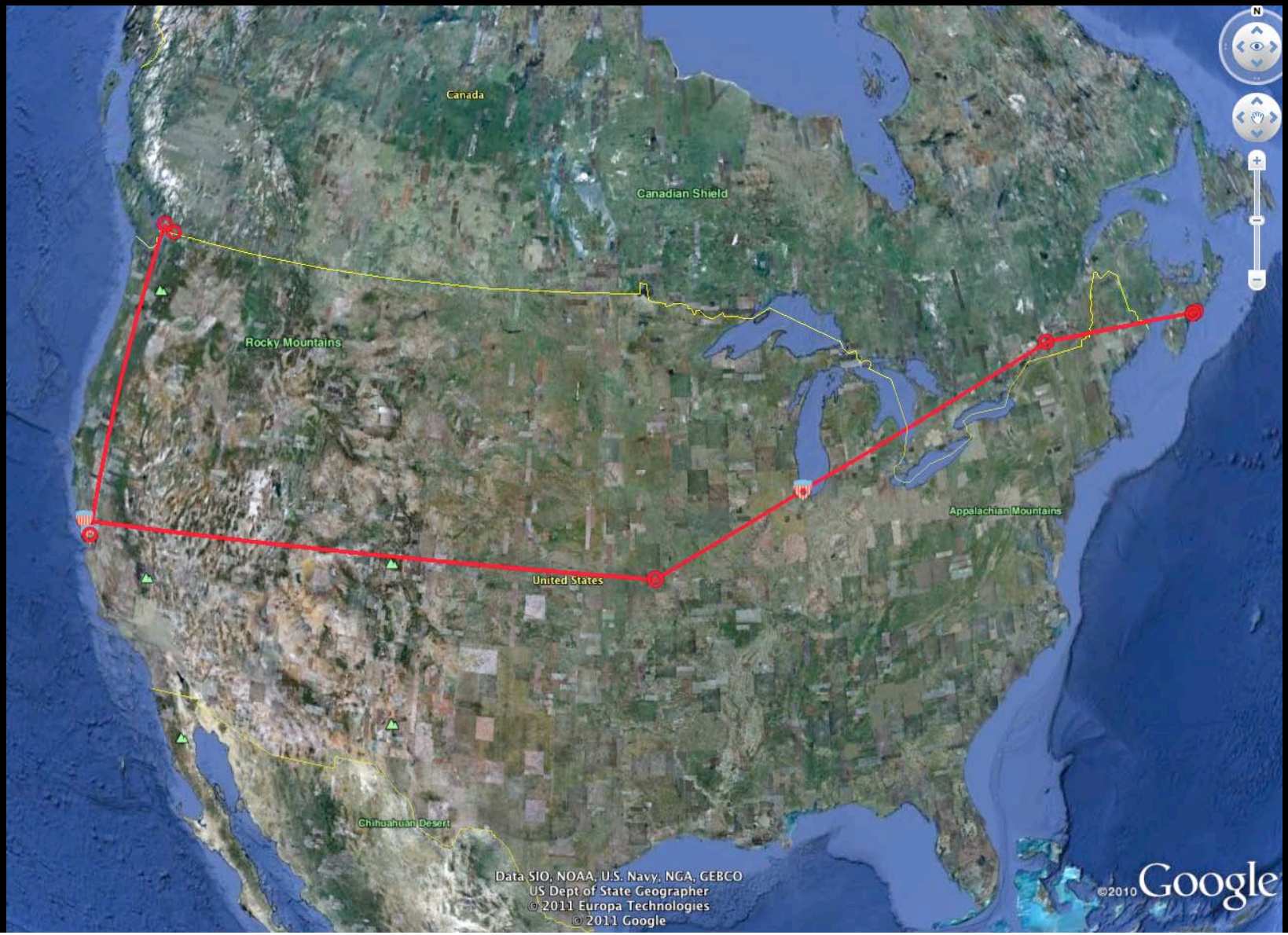
Traceroute id: **1751** Open in GoogleEarth
origin: **AustinTX** destination: **San Francisco CA** (sflawlib.ci.sf.ca.us [209.77.149.225])
submitter: AndrewC submitted: 2009-12-04 23:09

Hop	IP Address	Min. Latency	Carrier	Location	GeoPrecision	Hostname
1	12.231.120.0	0	AT&T WorldNet Services	Austin TX	Maxmind	12.231.120.0
2	12.89.72.5	0	AT&T WorldNet Services	Thrall TX	Maxmind	12.89.72.5
3	12.123.18.134	46	AT&T WorldNet Services	Dallas TX	city level	cr2.dlstx.ip.att.net
4	12.122.28.178	46	AT&T WorldNet Services	Los Angeles CA	city level	cr2.la2ca.ip.att.net
5	12.122.2.165	46	AT&T WorldNet Services	Los Angeles CA	city level	cr1.la2ca.ip.att.net
6	12.122.3.121	46	AT&T WorldNet Services	San Francisco CA	city level	cr1.sffca.ip.att.net
7	12.83.59.9	46	AT&T WorldNet Services	San Francisco CA	city level	12.83.59.9
8	151.164.38.26	46	AT&T Internet Services	San Francisco CA	city level	151.164.38.26
9	151.164.243.94	46	AT&T Internet Services	San Francisco CA	city level	ded1-g1-3-0.snfcca.sbcglobal.net
10	64.168.74.38	46	AT&T Internet Services	San Francisco CA	city level	VIP-CALNET-CCSF-Internet-City-1161485.cust-rtr.pacbell.net
11	208.121.241.249	47	CCSF	San Francisco CA	Maxmind	sf208-121-241-249.sfgov.org
12	209.77.149.225	47	CCSF	San Francisco CA	Maxmind	sflawlib.ci.sf.ca.us

Legend

- NSA: Known NSA listening facility in the city
- NSA: Suspected NSA listening facility in the city
- Hotel: Carrier hotel exchange point

Abbotsford BC > Halifax NS
Telus > Cogent > DalhousieU (TR1486)



Abbotsford BC > Halifax NS
Telus > Cogent > DalhousieU (TR1486)

Traceroute detail

Traceroute id: **1486**
origin: **V2T 5A5** destination: **Halifax NS** (www.dal.ca [129.173.1.241])
submitter: Mark submitted: 2009-12-01 19:43

Open in GoogleEarth

Hop	IP Address	Min. Latency	Carrier	Location	GeoPrecision	Hostname
1	205.250.64.0	0	Telus	Abbotsford BC	Maxmind	d205-250-64-0.bchsia.telus.net
2	154.11.88.193	0	Telus	Vancouver BC	city level	VANCBC01GR01
3	154.11.10.74	31	Telus	San Jose CA	city level	154.11.10.74
4	154.11.2.54	31	Telus	San Jose CA	city level	154.11.2.54
5	66.28.4.49	31	Cogent	San Jose CA	city level	te3-2.mpd01.sjc04.atlas.cogentco.com
6	154.54.7.173	31	Cogent	San Francisco CA	city level	te8-2.ccr02.sfo01.atlas.cogentco.com
7	154.54.24.118	63	Cogent	Kansas City MO	city level	te9-2.ccr02.mci01.atlas.cogentco.com
8	154.54.7.166	79	Cogent	Chicago IL	city level	te8-2.mpd02.ord01.atlas.cogentco.com
9	66.28.4.58	93	Cogent	Montreal QC	city level	te7-7.mpd01.ymq02.atlas.cogentco.com
10	38.104.154.162	109	Cogent	Lawrencetown NS	city level	38.104.154.162
11	198.166.1.41	109	Dalhousie University	Halifax NS	Maxmind	GigaPOP-gw.acorn-ns.Ca
12	198.166.1.18	109	Dalhousie University	Halifax NS	Maxmind	dal-gw.Backbone.Dal.Ca
13	129.173.1.241	109	Dalhousie University	Halifax NS	Maxmind	kil-ws-2.UCIS.Dal.Ca

Legend

- NSA: Known NSA listening facility in the city
- NSA: Suspected NSA listening facility in the city
- Hotel: Carrier hotel exchange point

Network sovereignty –
A Canadian perspective

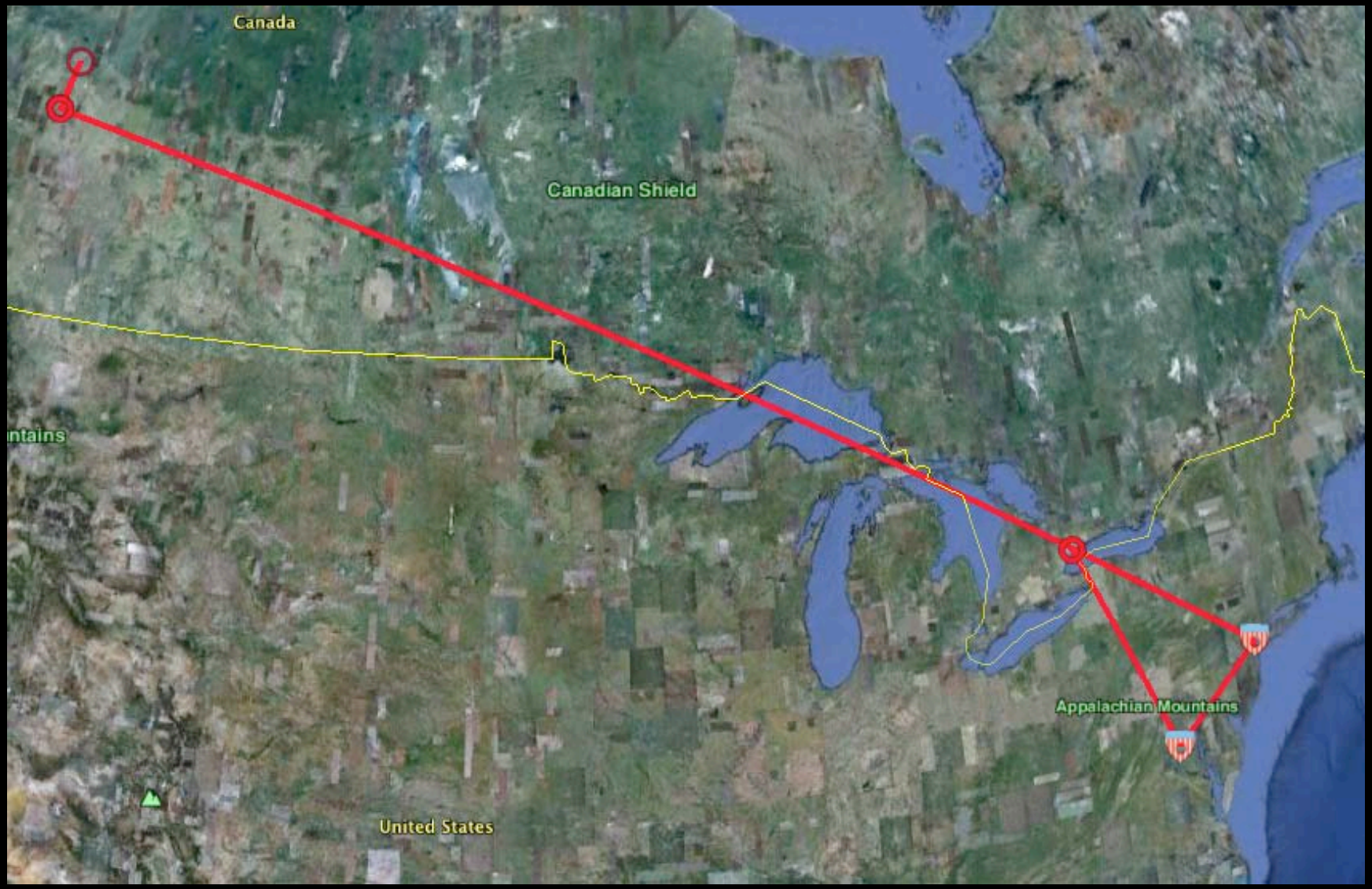
- Surveillance and privacy
  - Internet traffic via US routes or carriers brings exposure to USA PATRIOT Act and possibly NSA wiretapping
    - eg RefWorks case
- Cyber-infrastructure security
- Economic implications
- …

"Boomerang" routes

- Routes originate and terminate in Canada, but transit the US
- How common?
- Why?
  - Capacity/congestion? Least cost? Carrier interconnection policies?
- Implications?

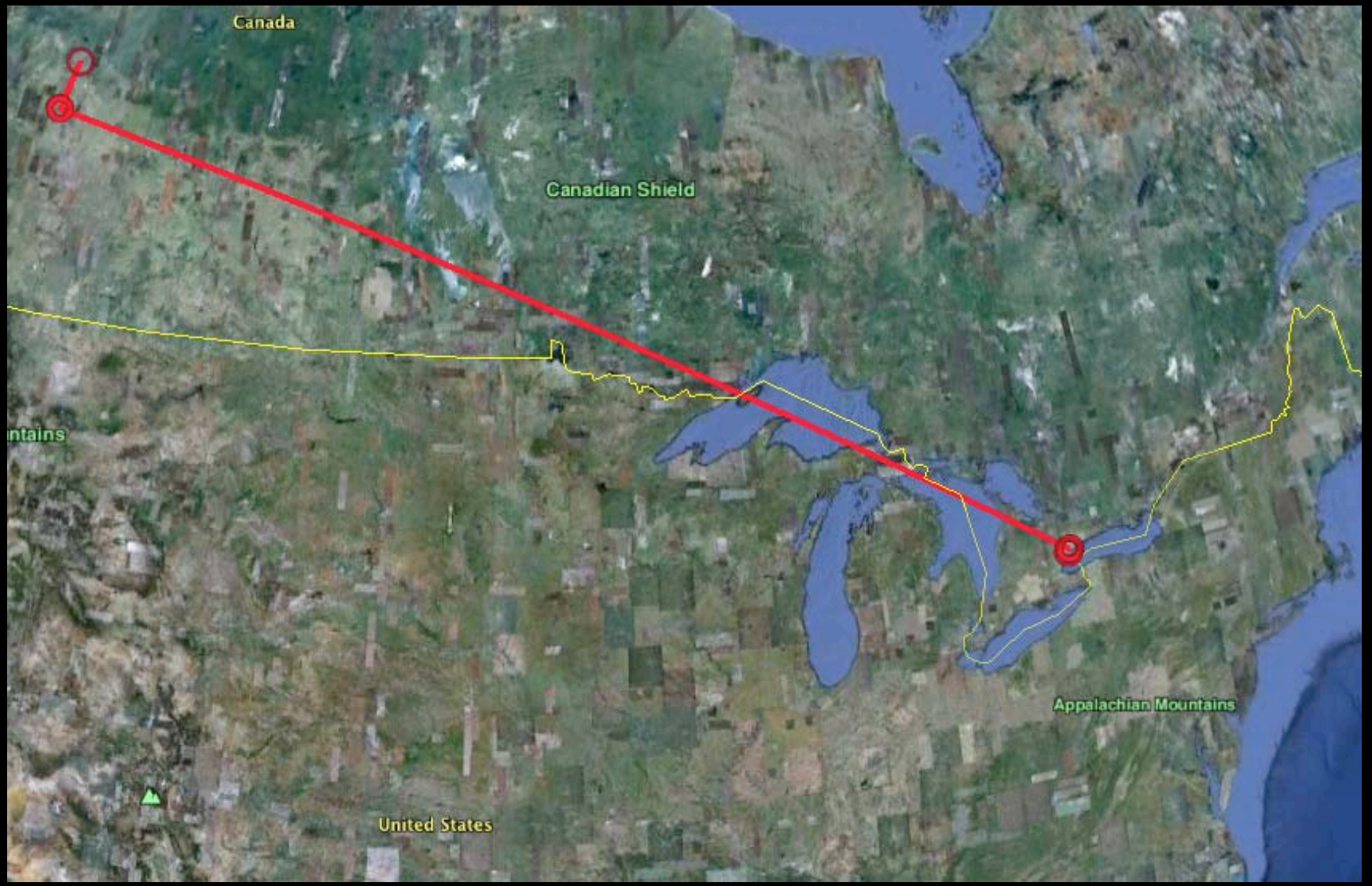
T.O. > AthabascaU

Teksavvy > Tiscali > Telus (TR4)

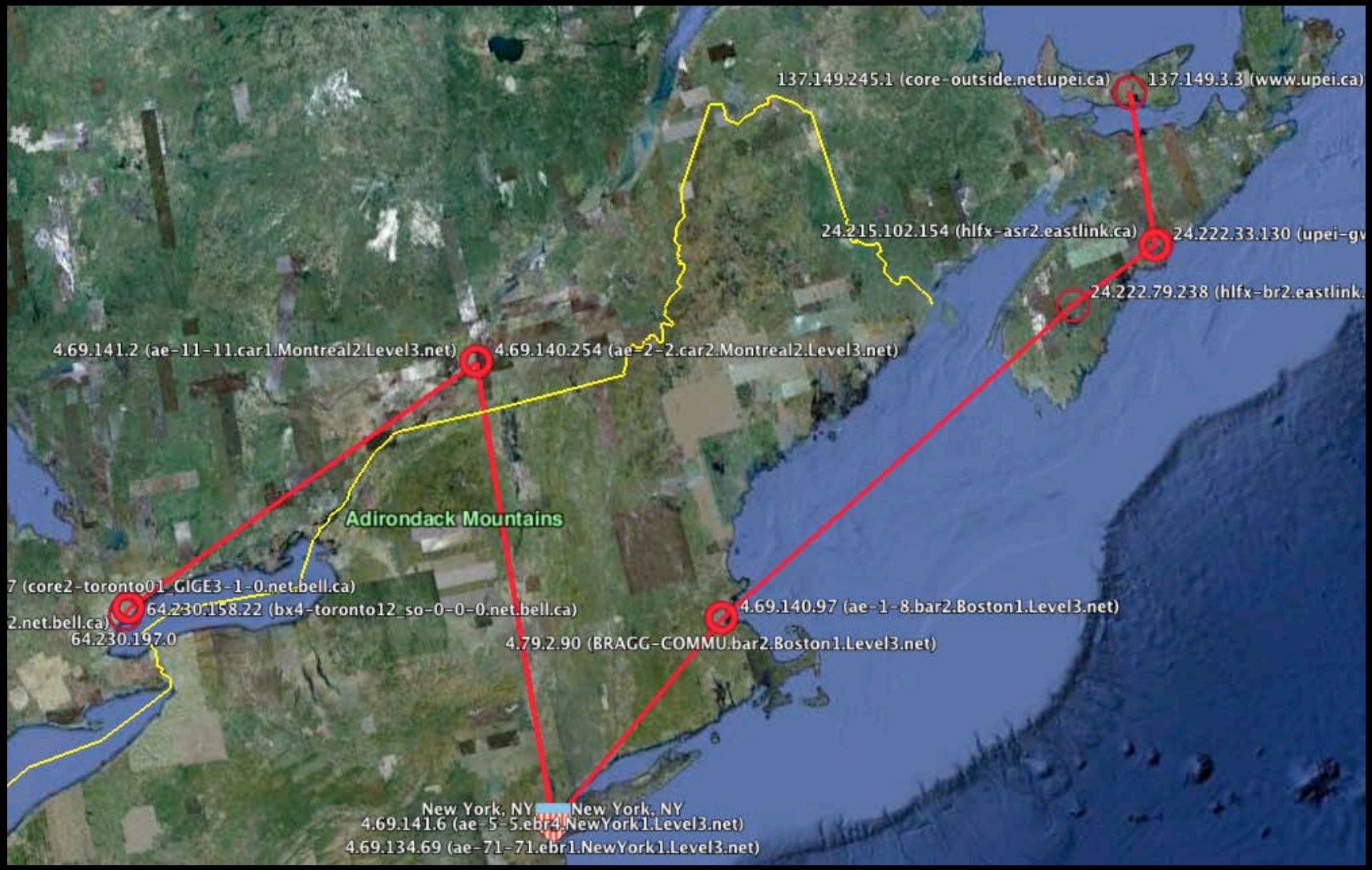


T.O. > AthabascaU

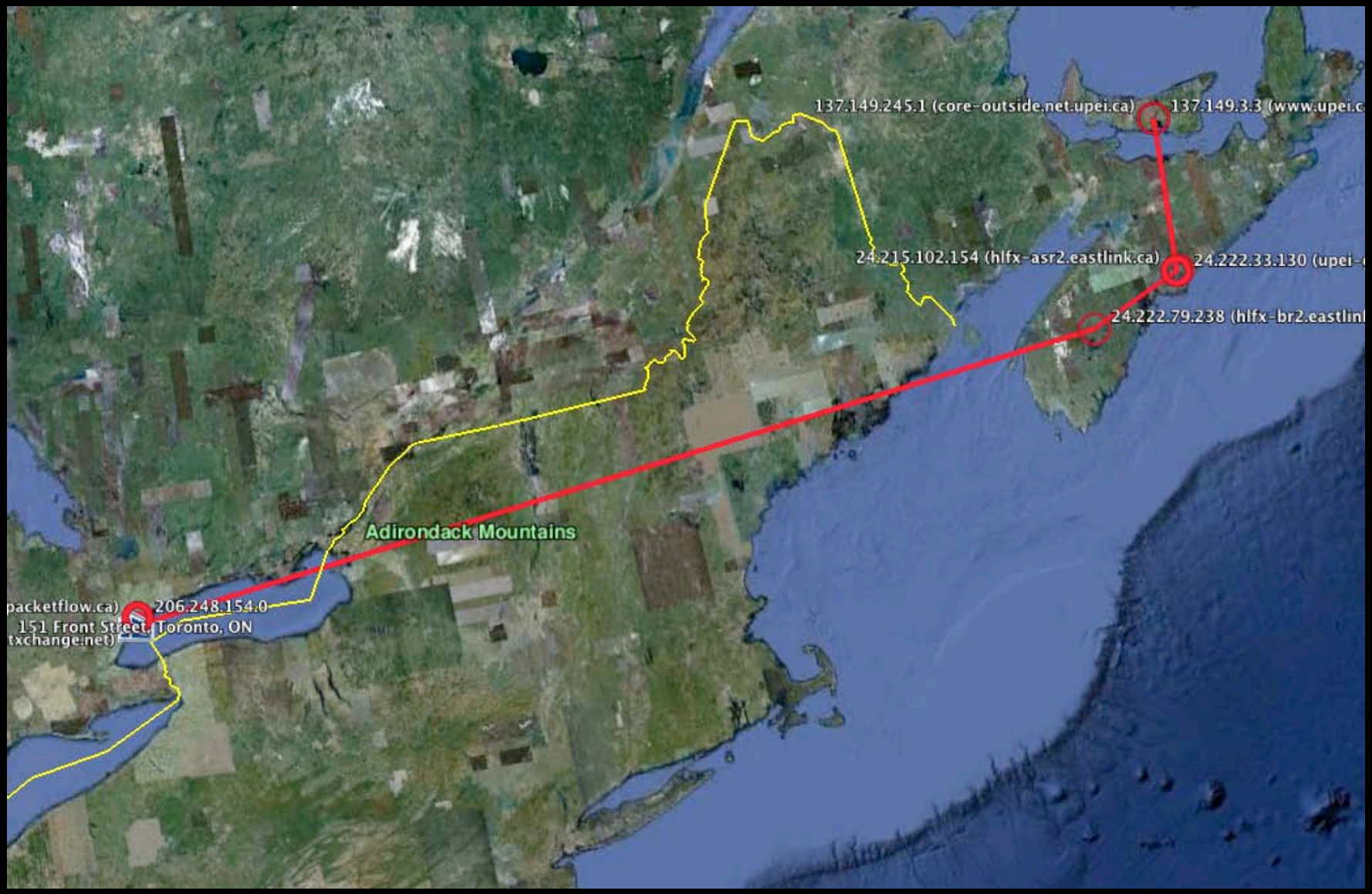
Bell > Telus (TR124)



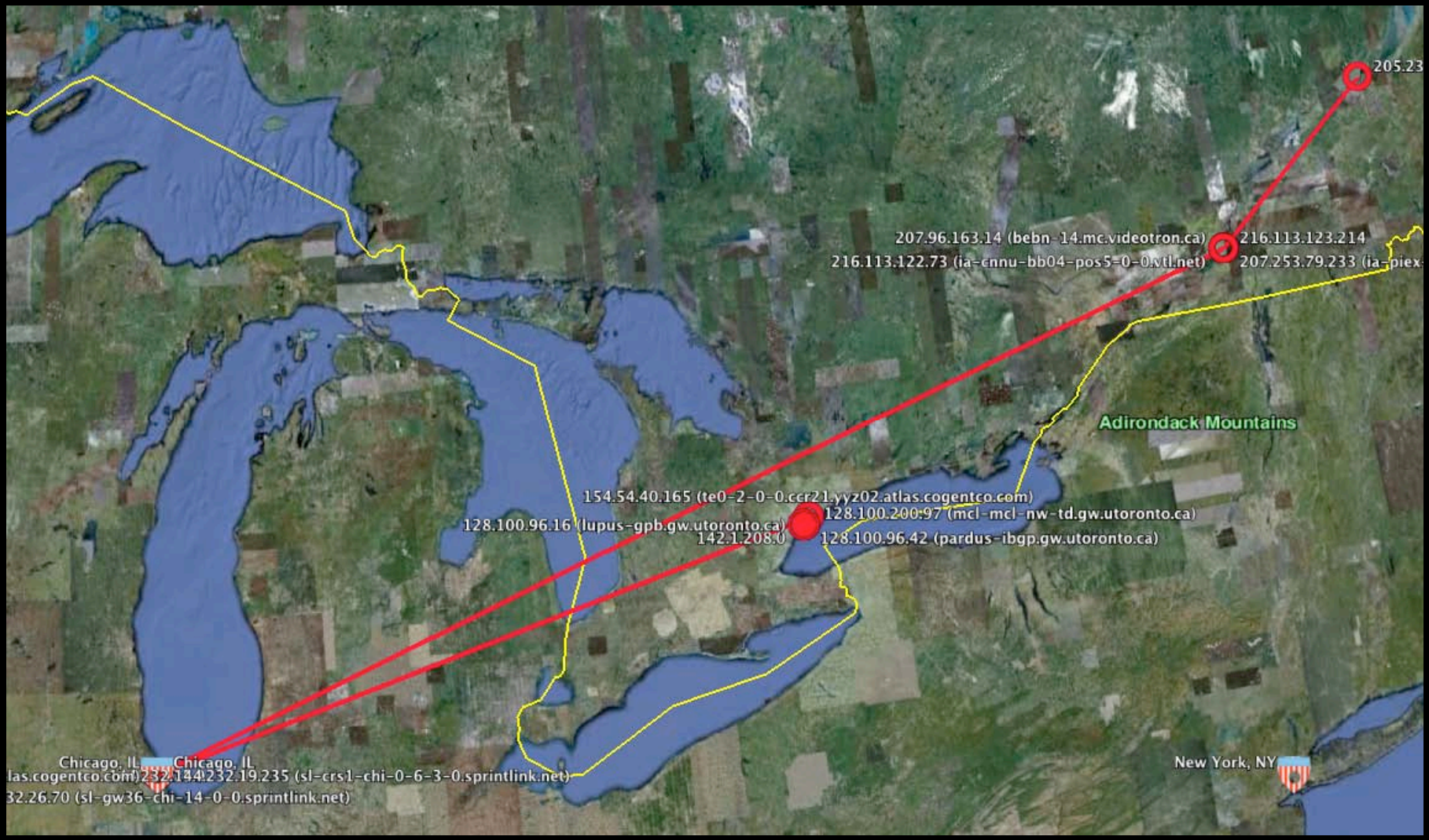
T.O. > PEI: Bell > Level3 > Eastlink (TR138)



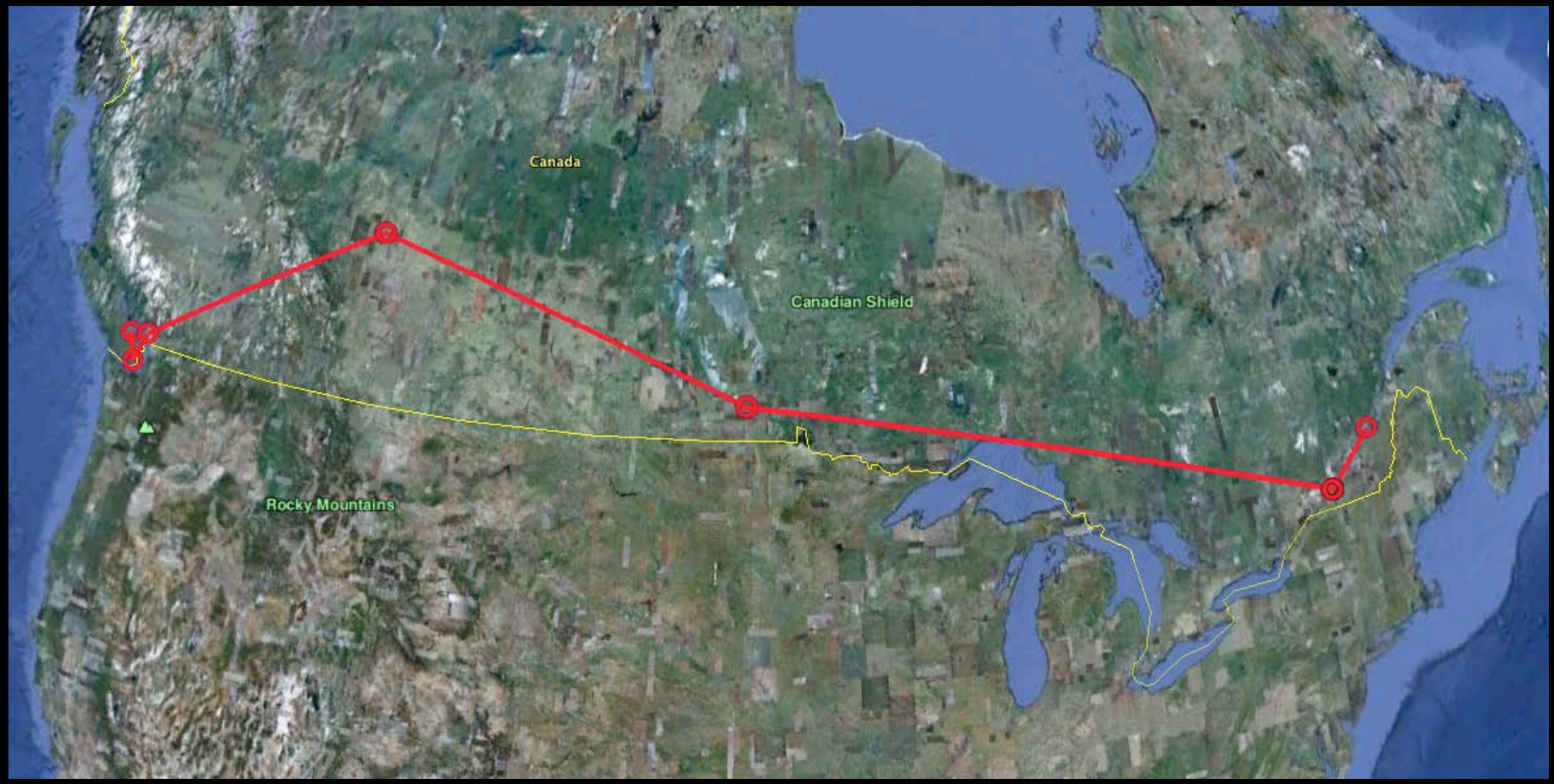
T.O. > PEI: Teksavvy > Eastlink (TR935)



T.O> Quebec City: UToronto> Cogent>Sprint>Videotron (TR7518)

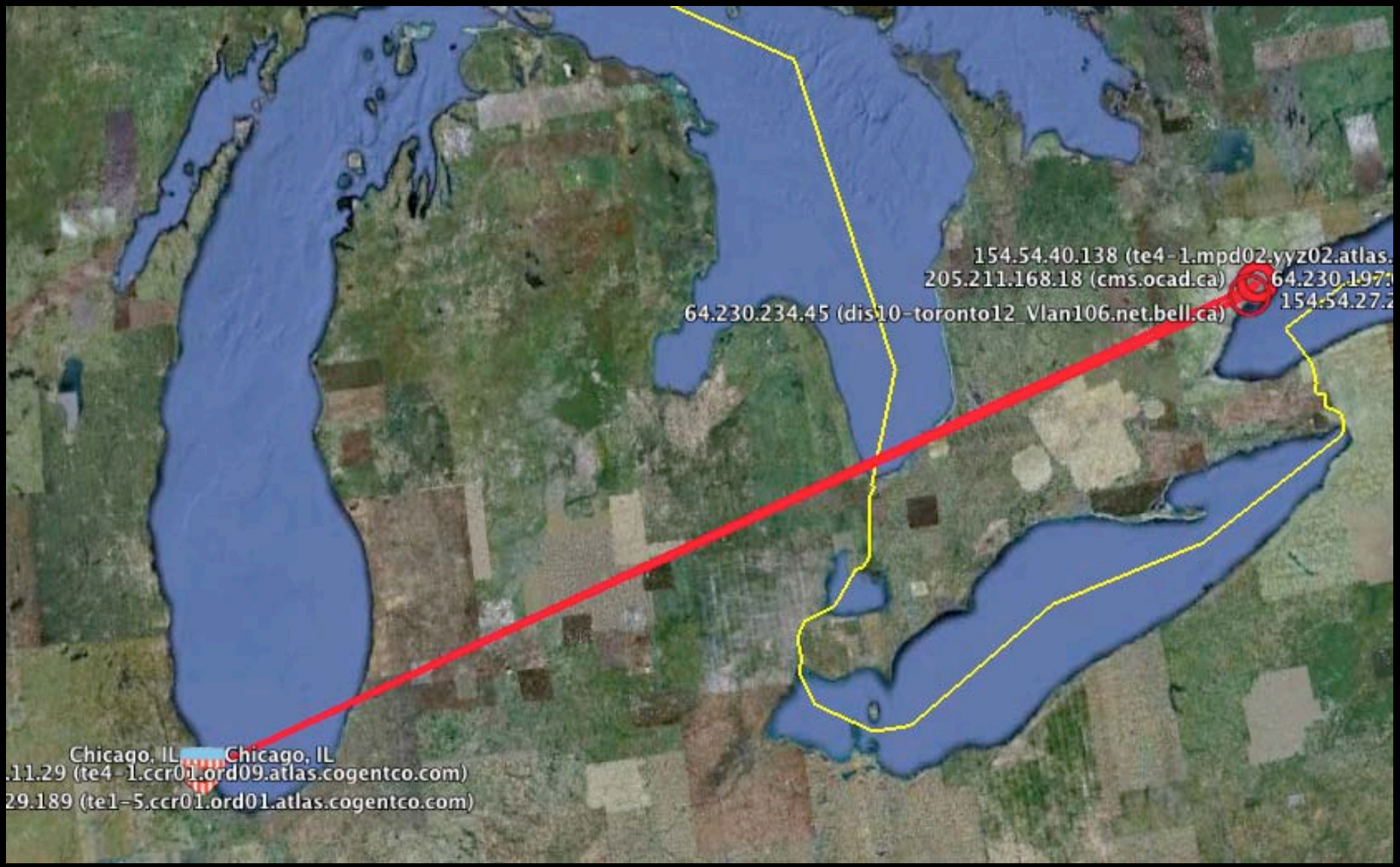


Nanaimo BC > Quebec City:
Shaw > Videotron (TR1204)



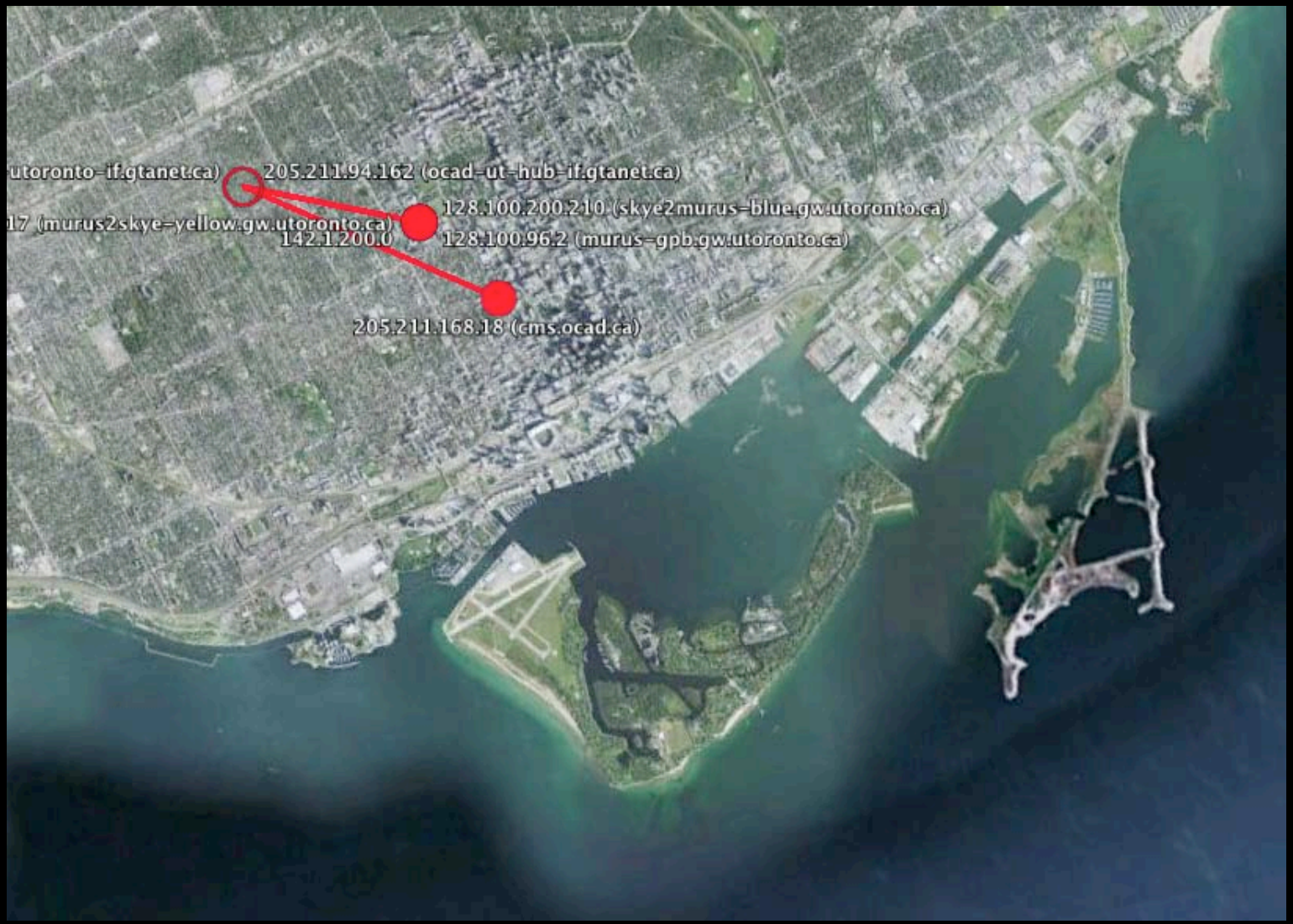
T.O. > T.O.(OCAD)

Bell > Cogent > GTAnet (TR6828)



T.O. > T.O.(OCAD)

UToronto > GTAnet (TR4158)



Findings (Preliminary)

- Canadian boomerang routing is commonplace (1/3 IXmaps)
- Canadian boomerang routing is largely related to interconnection policies, not capacity/congestion
  - If originating or terminating carrier is a major carrier, even a ‘competitor’, routing generally stays in Canada
- Major Canadian carriers (Bell, Telus, Videotron …) avoid connecting with smaller Canadian carriers in Canada
  - Requires use of foreign carriers for non-local transfers
  - Exchanges often occur in US
  - Brings heightened interception and surveillance risks
- Caveats:
  - Haven’t investigated relative costs
  - Needs more systematic collection of traceroute data, across location, time and carrier.

Implications

- Internet routing is a public interest concern
  - “Lawful access” legislation pending
- Public education
  - Internet traffic visualization tools/routing options
- Need for greater operational transparency by carriers
- Investigate privacy risks and protections
- Investigate possible oligopolistic behaviour?
- Promote greater interconnection among Canadian carriers within Canada

More information at http://IXmaps.ca

References:

- Bamford, James (2008) *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America*. Doubleday.
- Klein, Mark (2009) *Wiring Up The Big Brother Machine...And Fighting It.* Booksurge.
- Landau, Susan (2011) *Surveillance or Security? The Risks Posed by New Wiretapping Technologies*, MIT Press.