IXmaps

Tracking your Information Packets Over the Net, Through Exchange Points and Across Borders

Andrew Clement (U of T), Colin McCann (U of T), Gabby Resch (U of T), Erik Stewart (Independent)

iConference

Culture ♦ Design ♦ Society

Hosted by the Faculty of Information
University of Toronto
February 10, 2012
Today's Workshop

1. Enable attendees to learn about internet traceroute visualization, and in particular how they can use the IXmaps.ca mapping service to see where their packets travel, discovering information about ‘interesting’ points and internet policy issues along the way.

2. Enroll contributors in the collaborative expansion and refinement of the IXmaps.ca database of traceroutes, backbone router locations, and internet exchange point facts.

We hope to foster an enthusiastic cohort of informed individuals interested in collaboratively shedding light on the inner workings of the internet and contributing to the value and utility of the IXmaps tool.
1. Introductions (10 mins)
2. Motivations – backbone surveillance, network sovereignty (10mins)
3. Traceroutes and geolocating backbone routers (10 mins)
4. Traceroutes, visualization, IXmaps generation of TRs (30 mins)
5. Policy implications (20 mins)
6. Wrapup: staying in touch (10 mins)
Motivations
There is a popular tendency to regard the internet core as an immaterial, virtual, placeless 'cloud' where much happens, but without wider interest or concern.

The IXmaps research project seeks to dispel this myth by revealing the internet core’s political, geographical and physical concreteness.

It does this by illuminating for users the routes their packets take through the internet core along with the related issues - e.g. surveillance, ownership, network sovereignty, etc.
‘Inside’ the Internet

• 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 national security agencies)
  ○ Deep packet inspection (DPI) by ISPs/carriers
  ○ Discriminatory traffic management and blockage
  ○ Reach, reachability & (de-)peering
  ○ Cross-border flows (national “network sovereignty” issue)
  ○ Oligopolistic and anti-competitive business practices
  ○ Energy (over) consumption…

• ‘Cloud computing’ as a metaphor obscures important insights and possibilities for action
IXmaps Description

- IXmaps allows users to explore geographic visualizations of the routes taken by their information requests over the internet - presenting information about internet exchange points along the way. Data packet routes and switching sites are shown using Google Earth.
- The IXmaps project relies on voluntary user contributions to its database, mainly through the installation of TRgen, a modified version of a common Traceroute analysis program.
What is a traceroute?

- traceroute is a cross-platform network analysis tool, which shows the steps that data packets take to reach a target URL.

- To run, open a terminal and type:
  Mac – traceroute google.ca
  Windows – tracert google.ca
  Linux – traceroute google.ca

- Def'n: IP address – a number assigned to each device in a computer network, i.e. 172.168.4.28
Anatomy of a traceroute

<table>
<thead>
<tr>
<th>Hop</th>
<th>Hostname</th>
<th>IP Address</th>
<th>Latency</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.168.0.1</td>
<td>192.168.0.1</td>
<td>0.526 ms, 0.496 ms, 0.477 ms</td>
</tr>
<tr>
<td>2</td>
<td>7.6.80.1</td>
<td>7.6.80.1</td>
<td>11.938 ms, 11.936 ms, 11.919 ms</td>
</tr>
<tr>
<td>3</td>
<td>gw03.ktgc.phub.net.cable.rogers.com</td>
<td>66.185.89.129</td>
<td>12.762 ms</td>
</tr>
<tr>
<td>4</td>
<td>69.63.248.237</td>
<td>69.63.248.237</td>
<td>15.216 ms, 15.191 ms, 15.176 ms</td>
</tr>
<tr>
<td>5</td>
<td>so-0-3-0.gw02.bloor.phub.net.cable.rogers.com</td>
<td>66.185.80.202</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>tel-5.mpd01.iad01.atlas.cogentco.com</td>
<td>154.54.12.89</td>
<td>31.352 ms</td>
</tr>
<tr>
<td>7</td>
<td>te0-1-0-6.ccr21.iad02.atlas.cogentco.com</td>
<td>154.54.31.225</td>
<td>27.73 ms</td>
</tr>
<tr>
<td>8</td>
<td>te0-1-0-5.ccr21.dca01.atlas.cogentco.com</td>
<td>154.54.26.129</td>
<td>26.90 ms</td>
</tr>
<tr>
<td>9</td>
<td>te0-6-0-1.ccr21.jfk02.atlas.cogentco.com</td>
<td>66.28.4.125</td>
<td>39.836 ms, 741 ms</td>
</tr>
<tr>
<td>10</td>
<td>te0-2-0-3.ccr21.yyz02.atlas.cogentco.com</td>
<td>154.54.36.70</td>
<td>34.986 ms, 559 ms</td>
</tr>
<tr>
<td>11</td>
<td>te4-1.mpd02.yyz02.atlas.cogentco.com</td>
<td>154.54.40.138</td>
<td>34.941 ms</td>
</tr>
<tr>
<td>12</td>
<td>university-of-toronto.demarc.cogentco.com</td>
<td>38.117.74.226</td>
<td>33.06 ms</td>
</tr>
<tr>
<td>13</td>
<td>mcl-gpb.gw.utoronto.ca</td>
<td>128.100.96.7</td>
<td>32.656 ms, 31.683 ms, 34 ms</td>
</tr>
<tr>
<td>14</td>
<td>info-v1.utcc.utoronto.ca</td>
<td>128.100.72.45</td>
<td>33.617 ms, 33.583 ms</td>
</tr>
</tbody>
</table>
TRgen in action
TRgen in action (cont'd)
## Traceroute detail

Traceroute id: **7598**  
origin: **M4L**  
destination: **Toronto ON** (www.utoronto.ca [128.100.72.45])  
submitter: gbby_lville  
submitted: 2011-10-05 23:23

<table>
<thead>
<tr>
<th>Hop</th>
<th>IP Address</th>
<th>Min. Latency</th>
<th>Carrier</th>
<th>Location</th>
<th>GeoPrecision</th>
<th>Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>7.5.140.0</td>
<td>8</td>
<td>not listed by Maxmind</td>
<td>unknown</td>
<td>Maxmind</td>
<td>7.5.140.0</td>
</tr>
<tr>
<td>2</td>
<td>66.185.89.201</td>
<td>10</td>
<td>ROGERS-CABLE - Rogers Cable Communications Inc.</td>
<td>unknown</td>
<td>Maxmind</td>
<td>66.185.89.201</td>
</tr>
<tr>
<td>3</td>
<td>69.63.252.222</td>
<td>10</td>
<td>ROGERS-CABLE - Rogers Cable Communications Inc.</td>
<td>unknown</td>
<td>Maxmind</td>
<td>69.63.252.222</td>
</tr>
<tr>
<td>4</td>
<td>69.63.248.141</td>
<td>20</td>
<td>ROGERS-CABLE - Rogers Cable Communications Inc.</td>
<td>Chicago IL</td>
<td>city level</td>
<td>69.63.248.141</td>
</tr>
<tr>
<td>5</td>
<td>154.54.10.229</td>
<td>22</td>
<td>Cogent</td>
<td>Chicago IL</td>
<td>city level</td>
<td>te0-3-0-1.ccr21.ord03.atlas.cogentco.com</td>
</tr>
<tr>
<td>6</td>
<td>154.54.2.93</td>
<td>22</td>
<td>Cogent</td>
<td>Chicago IL</td>
<td>city level</td>
<td>te1-1.mpdo1.ord01.atlas.cogentco.com</td>
</tr>
<tr>
<td>7</td>
<td>154.54.27.250</td>
<td>22</td>
<td>Cogent</td>
<td>Chicago IL</td>
<td>city level</td>
<td>te8-1.mpdo1.yyz02.atlas.cogentco.com</td>
</tr>
<tr>
<td>8</td>
<td>154.54.43.173</td>
<td>22</td>
<td>Cogent</td>
<td>Toronto ON</td>
<td>city level</td>
<td>te0-2-0-0.ccr22.yyz02.atlas.cogentco.com</td>
</tr>
<tr>
<td>9</td>
<td>154.54.40.166</td>
<td>23</td>
<td>Cogent</td>
<td>Toronto ON</td>
<td>city level</td>
<td>te4-2.mpdo2.yyz02.atlas.cogentco.com</td>
</tr>
<tr>
<td>10</td>
<td>38.117.74.226</td>
<td>23</td>
<td>Cogent</td>
<td>Toronto ON</td>
<td>building level</td>
<td>university-of-toronto.demarc.cogentco.com</td>
</tr>
<tr>
<td>11</td>
<td>128.100.96.7</td>
<td>23</td>
<td>University of Toronto</td>
<td>Toronto ON</td>
<td>building level</td>
<td>mcl-gpb.gw.utoronto.ca</td>
</tr>
<tr>
<td>12</td>
<td>128.100.72.45</td>
<td>40</td>
<td>University of Toronto</td>
<td>Toronto ON</td>
<td>building level</td>
<td>info-v1.utcc.utoronto.ca</td>
</tr>
</tbody>
</table>

**Legend**
- NSA: Known NSA listening facility in the city
- NSA: Suspected NSA listening facility in the city
- Hotel: Carrier hotel exchange point
Geolocation of routers

- www.maxmind.com
- Free GeoLite service claims to locate “over 99.5% on a country level and 79% on a city level”
- Edge routers vs core routers
IXmaps geolocation methods - hostnames

colin@colin-W520:~$ traceroute www.utoronto.ca
traceroute to www.utoronto.ca (128.100.72.45), 30 hops max, 60 byte packets
1 192.168.0.1 (192.168.0.1) 0.526 ms 0.496 ms 0.477 ms
2 17.6.80.1 (17.6.80.1) 11.938 ms 11.936 ms 11.919 ms
3 gw03.ktgc.phub.net.cable.rogers.com (66.185.89.129) 12.762 ms
4 69.63.248.237 (69.63.248.237) 15.216 ms 15.191 ms 15.176 ms
5 so-0-3-0.gw02.bloor.phub.net.cable.rogers.com (66.185.80.202)
6 te1-5.mp01.iad01.atlas.cogentco.com (154.54.12.89) 31.352 ms
7 te0-1-0-6.ccr21.iad02.atlas.cogentco.com (154.54.31.225) 27.73078 ms
8 te0-1-0-5.ccr21.dca01.atlas.cogentco.com (154.54.26.129) 26.90078 ms
9 te0-6-0-1.ccr21.jfk02.atlas.cogentco.com (66.28.4.125) 39.836741 ms
10 te0-2-0-3.ccr21.yyz02.atlas.cogentco.com (154.54.36.70) 34.986559 ms
11 te4-1.mp02.yyz02.atlas.cogentco.com (154.54.40.138) 34.941 ms
12 university-of-toronto.demarc.cogentco.com (38.117.74.226) 33.0 ms
13 mcl-gpb.gw.utoronto.ca (128.100.96.7) 32.656 ms 31.683 ms 34 ms
14 info-v1.utcc.utoronto.ca (128.100.72.45) 33.617 ms 33.583 ms
### IXmaps geolocation methods - latency

**Traceroute detail**

Traceroute id: **7598**  
origin: M4L  
destination: **Toronto ON** (www.utoronto.ca [128.100.72.45])  
submitter: gbby_lville  
submitted: 2011-10-05 23:23

<table>
<thead>
<tr>
<th>Hop</th>
<th>IP Address</th>
<th>Min. Latency</th>
<th>Carrier</th>
<th>Location</th>
<th>GeoPrecision</th>
<th>Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>7.5.140.0</td>
<td>8</td>
<td>not listed by Maxmind</td>
<td>unknown</td>
<td>Maxmind</td>
<td>7.5.140.0</td>
</tr>
<tr>
<td>2</td>
<td>66.185.89.201</td>
<td>10</td>
<td>ROGERS-CABLE - Rogers Cable Communications Inc.</td>
<td>unknown</td>
<td>Maxmind</td>
<td>66.185.89.201</td>
</tr>
<tr>
<td>3</td>
<td>69.63.252.222</td>
<td>10</td>
<td>ROGERS-CABLE - Rogers Cable Communications Inc.</td>
<td>unknown</td>
<td>Maxmind</td>
<td>69.63.252.222</td>
</tr>
<tr>
<td>4</td>
<td>69.63.248.141</td>
<td>20</td>
<td>ROGERS-CABLE - Rogers Cable Communications Inc.</td>
<td>city level</td>
<td>Maxmind</td>
<td>69.63.248.141</td>
</tr>
<tr>
<td>5</td>
<td>154.54.10.229</td>
<td>22</td>
<td>Cogent</td>
<td>city level</td>
<td>te0-3-0-1.ccr21.ord03.atlascogentco.com</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>154.54.2.93</td>
<td>22</td>
<td>Cogent</td>
<td>city level</td>
<td>te1-1.mpdo1.ord01.atlascogentco.com</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>154.54.27.250</td>
<td>22</td>
<td>Cogent</td>
<td>city level</td>
<td>te8-1.mpdo1.yyz02.atlascogentco.com</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>154.54.43.173</td>
<td>22</td>
<td>Cogent</td>
<td>city level</td>
<td>te0-2-0-0.ccr22.yyz02.atlascogentco.com</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>154.54.40.166</td>
<td>23</td>
<td>Cogent</td>
<td>city level</td>
<td>te4-2.mpdo2.yyz02.atlascogentco.com</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>38.117.74.226</td>
<td>23</td>
<td>Cogent</td>
<td>building level</td>
<td>university-of-toronto.demarc.cogentco.com</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>128.100.96.7</td>
<td>23</td>
<td>University of Toronto</td>
<td>building level</td>
<td>mcl-gpb.gw.utoronto.ca</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>128.100.72.45</td>
<td>40</td>
<td>University of Toronto</td>
<td>building level</td>
<td>info-v1.utcc.utoronto.ca</td>
<td></td>
</tr>
</tbody>
</table>
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)
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.
Chicago: 350E Cermak Rd.
San Francisco: 611 Folsom St

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 941A, an intercept facility operated by AT&T for the NSA, was documented by former network engineer and whistleblower, Mark Klein.
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)
EFF's view:

Source: Electronic Frontier Foundation (EFF)
Suspected NSA surveillance sites
New York, NY > San Francisco, CA
Can coast-to-cost US traffic avoid NSA cities?

So far as we’ve seen, no!
Traceroutes Generation and Visualization
Austin TX > San Francisco Law Library, SF CA (TR1751)
## Traceroute detail

Traceroute id: 1751

**origin**: Austin TX  **destination**: San Francisco CA (sfawlib.ci.sf.ca.us [209.77.149.225])

**submitter**: AndrewC  **submitted**: 2009-12-04 23:09

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

**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)
**Traceroute detail**

Traceroute id: 1486  
Origin: V21 SAS  
Destination: DalhousieU (TR1486)  
Submitter: Mark  
Submitted: 2009-12-01 19:43

<table>
<thead>
<tr>
<th>Hop</th>
<th>IP Address</th>
<th>Min. Latency</th>
<th>Carrier</th>
<th>Location</th>
<th>GeoPrecision</th>
<th>Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>203.250.64.0</td>
<td>0</td>
<td>Telus</td>
<td>Abbotsford BC</td>
<td>Maxmind</td>
<td>d205-250-64-0.bchsi.telus.net</td>
</tr>
<tr>
<td>2</td>
<td>154.11.88.193</td>
<td>0</td>
<td>Telus</td>
<td>Vancouver BC</td>
<td></td>
<td>VANCBC01GR01</td>
</tr>
<tr>
<td>3</td>
<td>154.11.10.74</td>
<td>31</td>
<td>Telus</td>
<td>San Jose CA</td>
<td></td>
<td>154.11.10.74</td>
</tr>
<tr>
<td>4</td>
<td>154.11.2.54</td>
<td>31</td>
<td>Telus</td>
<td>San Jose CA</td>
<td></td>
<td>154.11.2.54</td>
</tr>
<tr>
<td>5</td>
<td>66.28.4.49</td>
<td>31</td>
<td>Cogent</td>
<td>San Francisco CA</td>
<td></td>
<td>te3-2.mpd01.sjc04.atlas.cogentco.com</td>
</tr>
<tr>
<td>6</td>
<td>154.54.7.173</td>
<td>31</td>
<td>Cogent</td>
<td>Kansas City MO</td>
<td></td>
<td>te8-2.ucr02.sfo01.atlas.cogentco.com</td>
</tr>
<tr>
<td>7</td>
<td>154.54.24.118</td>
<td>63</td>
<td>Cogent</td>
<td>Chicago IL</td>
<td></td>
<td>te9-2.ucr02.mci01.atlas.cogentco.com</td>
</tr>
<tr>
<td>8</td>
<td>154.54.7.166</td>
<td>79</td>
<td>Cogent</td>
<td>Montreal QC</td>
<td></td>
<td>te8-2.mpd02.mrd01.atlas.cogentco.com</td>
</tr>
<tr>
<td>9</td>
<td>66.28.4.58</td>
<td>93</td>
<td>Cogent</td>
<td>Lawrencetown NS</td>
<td></td>
<td>te7-7.mpd01.ymq02.atlas.cogentco.com</td>
</tr>
<tr>
<td>10</td>
<td>38.104.154.162</td>
<td>109</td>
<td>Cogent</td>
<td>Halifax NS</td>
<td>Maxmind</td>
<td>GigaPOP-gw.assign-ca.mca.ca</td>
</tr>
<tr>
<td>11</td>
<td>198.166.1.41</td>
<td>109</td>
<td>Dalhousie University</td>
<td>Halifax NS</td>
<td>Maxmind</td>
<td>dal-gw.Backbone.Dal.Ca</td>
</tr>
<tr>
<td>12</td>
<td>198.166.1.18</td>
<td>109</td>
<td>Dalhousie University</td>
<td>Halifax NS</td>
<td>Maxmind</td>
<td>Dalhousie University</td>
</tr>
</tbody>
</table>

**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? About 40% of routes that originate and terminate in Canada go through the US
- Why?
  - Capacity/congestion. Cost. Carrier interconnection policies.
- Implications
T.O. > T.O.(OCAD) U.Toronto > GTAnet (TR4158)
T.O. > T.O.(OCAD) Bell > Cogent > GTA.net (TR6828)
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)
The Internet Core
(in North America)

Bell
• bell.ca
• bellnexxia
• bellglobal
• sympathetic
Policy Implications
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.
'Lawful Access' legislation

C-50 (Improving Access to Investigative Tools for Serious Crimes Act)
• make it easier for the police to obtain judicial approval of multiple intercept and tracking warrants and production orders, to access and track e-communications.

C-51 (Investigative Powers for the 21st Century Act)
• give the police new powers to obtain court orders for remote live tracking, as well as suspicion-based orders requiring telecommunication service providers and other companies to preserve and turn over data of interest to the police.

C-52 (Investigating and Preventing Criminal Electronic Communications Act)
• require telecommunication service providers to build and maintain intercept capability into their networks for use by law enforcement, and gives the police warrantless power to access subscriber information.
Concerns

• Expands the scope and depth of surveillance
• Threatens fundamental rights and freedoms, most notably privacy
• Lack of justification
• Lack of public debate
• Lack of judicial oversight
• Lack of public accountability
• Lack of stringent conditions
• Builds surveillance capacity into the infrastructure

http://www.unlawfulaccess.net/
Implications

- Internet routing is a public interest concern
- Public education
  - Internet traffic visualization tools/routing options
- Promote greater operational transparency by carriers and service providers
- Investigate privacy risks and protections
- Investigate possible oligopolistic behaviour
- Promote traffic exchange within Canada
  - Challenge pending “lawful access” legislation
    - [http://openmedia.ca/StopSpying](http://openmedia.ca/StopSpying)
Implications

- Internet routing is a public interest concern
- 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
- Resist pending “Lawful Access” legislation
Wrapup
See where your packets go!
(and contribute to the database)

Try it out and get more information at:
http://IXmaps.ca
Project team:
- Andrew Clement,\textsuperscript{1} Steve Harvey,\textsuperscript{3} Yannet Lathrop,\textsuperscript{1} Colin McCann,\textsuperscript{1} Nancy Paterson,\textsuperscript{2} Gabby Resch\textsuperscript{1} & Erik Stewart\textsuperscript{3}
\textsuperscript{1} Faculty of Information, Univ of Toronto
\textsuperscript{2} OCAD University
\textsuperscript{3} Independent

Funding:
- Social Sciences and Humanities Research Council (SSHRC)

References:
- Klein, Mark (2009) \textit{Wiring Up The Big Brother Machine...And Fighting It}. Booksurge.