IXmaps: Interactively mapping NSA surveillance points in the internet "cloud"

by Andrew Clement, Nancy Paterson and David J. Phillips

Faculty of Information, University of Toronto

correspondence: andrew.clement@utoronto.ca

30 June 2010

This is a revision of a paper originally presented at the 'A Global Surveillance Society?' conference, City University, London UK, April 13-15, 2010 http://www.surveillancecultures.org/.

ABSTRACT

The rapidly growing deployment of networked digital media greatly expands the scope and intensity of everyday surveillance. This is well understood but the research into digital surveillance has largely concentrated on its more publicly visible aspects. Relatively little research has focused on surveillance carried out in the core of the internet. A rare exception to the prevailing obscurity of surveillance on the internet backbone was the revelation in 2006 of the 'warrantless wiretapping' program, in which the National Security Agency (NSA) installed 'splitter' rooms in several major internet exchange points. These secret surveillance sites route a replica of the entire packet stream to NSA computers for analysis and storage. In terms of scale of data collection this arguably constitutes one of the largest surveillance operations in history. It also represents among the most serious contemporary challenges to democratic governance and civil liberties.

Notwithstanding the publicity that has surrounded this controversial NSA wiretapping, there is little public or critical scholarly understanding of the socio-technical mechanics of this form of surveillance, nor its wider implications. As part of an on-going research program aimed at rendering more visible the hitherto hidden aspects of digitally mediated surveillance[1], the IXmaps research reported in this paper seeks to show internet users whether their internet communications passes through any of the approx 20 NSA wiretapping sites. This is done

[1] see http://www.surveillanceproject.org/about/IRSP_2

through a software package we have developed that displays on a map of North America the path taken by user-initiated data packets and which of the main internet exchange points along this path the NSA has most likely established splitter rooms. The software also shows other relevant information about the surveillance sites, such as exchange point ownership, telecom carrier connectivity, photos of the exchange building, court documents, news reports, and the like.

This paper discusses the development of the IXmaps software. In particular, we note the ways in which the internet makes visible activities at its periphery much more readily than activities at the core. We also the usefulness of IXmaps as a tool for achieving better public awareness of internet surveillance and other issues of internet governance.

INTRODUCTION

Mark Klein, a retired AT&T technician, touched off a storm of controversy in 2006 when he revealed that the U.S. National Security Agency (NSA) had secretly installed special facilities in AT&Ts main San Francisco internet exchange point that were capable of copying and analyzing potentially all the internet traffic passing through that location. It soon became clear that this was the tip of a much bigger iceberg, covering all forms of telecommunications traffic and implicating most of the main carriers across the U.S. What became known as the NSA warrantless surveillance controversy is arguably the largest single surveillance program conducted by a government over the communications of its citizens. Congressional passage of special legislation in 2008 to protect telecommunications carriers against the dozens of lawsuits that ensued largely ended media attention to the controversy, with the constitutional and civil liberties issues unresolved, and considerable mystery remaining about what actually happened. With no evidence to the contrary, it is highly likely that these surveillance activities continue, but with little public knowledge or understanding.

In addition to the obscurity that the security forces typically operate under, the challenge for public education about these widespread surveillance practices is compounded by the opacity of the inner workings of the internet and the popular imaginary of it as a "cloud". The IXmaps project seeks to address this lack of public understanding by rendering more visible the usually hidden workings of the internet core. In particular, this paper reports on how the IXmaps software operates, how its development revealed the techniques by which the opacity of "the cloud" is maintained, and how people can use and extend IXmaps to reveal how the cloud is grounded in issues of policy, property, and jurisdiction.

We begin by describing the NSA's alleged internet surveillance activities. To better understand how this interception is done, as well as how we can detect where it is taking place, we then provide a brief overview of the technical aspects of internet routing. The heart of the paper is an explanation of the IXMaps traceroute capture and mapping software that shows the path one's internet packets take across the internet, as well as "interesting" points along the way. Most notable among these are the locations where the NSA is alleged to have installed "splitter rooms" capable of intercepting one's communications. We close by identifying the current limitations and future directions of this approach to making the internet "cloud," and the activities within it, more publicly visible.

NSA'S WARRANTLESS SURVEILLANCE ACTIVITIES

Roughly four dozen court cases against U.S. telecom carriers allege that they illegally complied with multiple surveillance requests from the NSA during the Bush Adminstration. They specify three main types of request, for:

1. Detailed phone records (i.e. customer calling records revealing who called whom, when, but not revealing any of the content of the calls)
2. Monitoring of telephone calls (i.e. eavesdropping on the actual phone conversations, either live, or more usually, recording them for later analysis and listening - this has long been possible with conventional phone technology.
3. Installation of internet "splitter rooms", so that NSA can directly monitor all traffic at that point - email, web access, VoIP conversations, etc.

Though all three forms of request raise serious issues about the legality of the U.S. government's actions and the encroachment on civil liberties,[2] in this paper we are concerned primarily with the last of these – the mass replication of internet traffic. This is the most novel form of surveillance as well as the one with the greatest scope, depth and potential for incursion into an individual's activities.

The main charges are against AT&T as well as Verizon/MCI, BellSouth, Sprint, and Cingular.[3] These court cases are still pending, with the federal government seeking to have them dismissed on "national security" grounds. The FISA Amendments Act of 2008, popularly known as the "Telecom Immunity Act", may render these cases moot, as this legislation "allow[s] federal judges to waive lawsuits if the telecom firms can prove that they were authorized by the president and assured that the program was legal."[4]

Unlike the five telecom carriers facing lawsuits, Qwest reportedly did not comply with the NSA's request to turn in customers' telephone records. Moreover, Qwest CEO claims that this request was made in February 2001, well before the attacks of September 11. In addition to

[2] These three different activities are often conflated in the press coverage. Reporters aren't always careful to distinguish between the various forms of "eavesdropping" and use the term loosely.

[3] Refer to the Appendix for a summary of the charges.

[4] Soraghan, Mike. 2008. "House passes FISA overhaul" *The Hill,* June 20, 2008; and http://www.sourcewatch.org/index.php?title=FISA_Amendments_Act_of_2008

requests for phone records, Qwest was also approached by unnamed “clandestine agencies” about allowing the latter the use of Qwest's “fiber-optic communications network for government purposes.” Qwest did not comply.

In this paper, we focus on AT&T, and the splitter room installation at 611 Folsom Street in San Francisco, as this is the best documented case and provides a model for the interception of internet traffic at 15 to 20 other major internet exchange points in the U.S.[5] To understand the role that sites like 611 Folsom Street play, we turn now to a quick review of internet routing.

ROUTING PACKETS ACROSS THE INTERNET ‘BACKBONE’

Viewing a website or sending a message to a destination on the Internet involves two processes, naming and routing. In name resolution a domain name server (DNS) is queried with a the URL (or hostname) of the intended destination. DNS responds with the IP number associated with that hostname. IP numbers identify devices such as computers, servers and routers within the internet. IP numbers, rather than URLs or hostnames, are used in the actual routing of messages. Thus any device connected to the internet may have associated with it both a hostname (suitable for human mnemonics) and an IP address (for automated routing and addressing). IP addresses are allocated in blocks to major network providers who may in turn sub-allocate to smaller (end user access) network providers and/or end users (customers).

Data sent over the internet is typically sent in a series of small packets, each with a header, containing, among other items, source and destination IP addresses, much like the to and return addresses on a conventional piece of mail. Each packet is passed through data traffic routers, with each router passing the packets closer to the intended destination, again much like the conventional postal service routes mail. The destination, when reached, may return a response, whether it is a web page, video, file transfer, etc.

Packets usually travel from the end user’s computer to the routers of the user’s Internet Service Provider (ISP). The ISP the forwards them through a gateway router to the internet backbone or core. The packets travel through the core to the recipients’ ISP, then to the recipient herself. The core, which handles the bulk of long distance internet traffic, generally consists of

[5] Lichtblau, Eric. 2007. “Role of Telecom Firms in Wiretaps Is Confirmed” *New York Times (*August 24); http://www.nytimes.com/2007/08/24/washington/24nsa.html?ex=1345608000&en=4e8428cf3d46306c&ei=5090&partner=rssuserland&emc=rss

many high speed routers and high bandwidth data lines. These are generally owned and operated by national or international telecommunications companies.

The telecom companies operating the core manage their networks through "autonomous systems" (or "AS"s). An AS is an administrative and procedural policy for handling traffic through routers. Each core carrier uses its own AS (or set of AS's) to manage traffic within its network. In assigning an AS to a router, the carrier is instructing that router on the procedures it is to follow in routing packets. For the purposes of this paper, it is important to note only that the AS number assigned to each router is public, and that that AS number identifies the operator of the router as well as the policies that the router follows.

Despite popular nomenclature, the internet core does not have a single "backbone" in the traditional sense. Rather it is comprised of relatively distinct high speed, high bandwidth data networks of operated by approximately a dozen international commercial network providers. These global networks are interconnected at many different places, called 'peering points'. Bandwidth converges at peering points in order for data communications to be switched between networks to reach their final destinations. These peering points, or internet exchange points, are usually located in "carrier hotels" - very large multi-story office towers in major cities where the entire building is full of servers mounted in racks, massive electrical power, and heating and cooling. Bandwidth stakeholders may lease one rack or even several floors of the building. There is a central 'meet-me-room' where the various stakeholders physically cross-connect wires or fibre.

As Savageau describes them:

> Carrier hotels are by nature real estate operations. Carrier hotels make money by leasing or licensing footprint, uninterruptible power, cooling, and interconnections. The more interconnections and networks present within a property, the more important that property became to the telecom and network provider community. The reasoning is pretty simple. If you are in a carrier hotel you can generally interconnect with another network or carrier through use of a local cross connect, and in some cases simply a "jumper" cable. …A carrier hotel such as One Wilshire (in L.A.) may have more than 300 carriers and service providers present as tenants within a single building. Most of those tenants will have a direct presence

> within a building-operated meet-me-room, allowing all carriers easy access to one another as all are within close proximity. (n.d. p. 1)

The concept and practices of peering came to the attention of news media in early 2006 when Mark Klein, a retired ATT technician revealed that in 2002 he found evidence that the NSA had installed eavesdropping equipment at their internet exchange facilities at 611 Folsom Street in San Francisco (Bamford, 2008, pp.189-190; Young 2007).

Thus we can see that the "cloud" is amenable, at its core, both technically and administratively, to sophisticated, covert surveillance operations by national policing and intelligence agencies. One of the purpose of the IXMaps project is to continue to reveal these practices, or at least to reveal the socio-technical configurations that make them possible.

MAPPING PACKETS ACROSS THE INTERNET BACKBONE

We are now in a position to describe how the IXmaps software maps the routes taken by an individual's internet communications (whether an email, web request, VoIP call, etc.), and displays information about nodes along the route. IXMaps was intended in its inception to be a general purpose for displaying all kinds of information about the routes of internet packets. Depending on the interests of IXMaps users, this information might include the carriers operating each segment of the route, the location of the facilities in which routers and switches are housed, the owners of those facilities, and any connections those owners might have to national police, defense, or intelligence agencies.

The IXmaps platform consists of two major parts. The first is a software program called TRgen, which traces the route packets take from the users local machine to a given device on the internet. Based on the widely available 'traceroute' program,[6] TRgen automatically sends out a series of test packets to a set of destination addresses. Both TRgen and the destination set can downloaded from the IXmaps website and run by users from any location. When run, TRgen generates a sequence of IP addresses, starting with an anonymized local address, together with the times it takes packets to reach each of the intermediate routers on the way to the destination site. TRgen immediately stores these route sequences in a database on the IXmaps server. TRgen then augments the database by adding the AS number, the hostname, and latitude and longitude of each router in the route sequence. We obtained the AS numbers and hostnames from

[6] see http://en.wikipedia.org/wiki/Traceroute

the *whois* function of the American Registry for Internet Numbers (ARIN)[7]. The latitude and longitude information is commercially available via MaxMind's GeoLite database.[8] See Table 1 for an example based on a trace route between a home computer in Toronto Canada, with postal code of M5S2M8, to the San Francisco Art Institute, (http:sfai.edu) performed December 13, 2009.

In October 2009 we began inviting people to try out TRgen software and help us build the IXmaps database. We produced two sets of pre-defined destinations. One included about 30 URLs of universities located around the periphery of North America, and was intended to harvest traceroutes that collectively would transit most of the core internet routers. A second set with a similar number of sites located in San Francisco and the Bay Area we intended to target AT&T's known splitter room site at 611 Folsom St. By March 2010, the database included roughly 3000 traceroutes, initiated by about 30 individuals from more than that number of locations, mainly in Toronto as well as scattered around North America.

[7] see https://ws.arin.net/whois

[8] see http://maxmind.com/

<Begin Table 1>

Traceroute detail

id= **1859** GoogleEarth when=**2009-12-13 12:06** from=**M5S2M8** to=**sfai.edu [63.197.251.33]**

Hop	IP Address	Round Trip Times				AS#	Latitude	Longitude	Hostname
1	206.248.154.0	0	0	0	15	5645	42.4	-82.1833	206.248.154.0
2	69.196.136.66	0	*	0	0	5645	43.8667	-79.4333	2120.ae0.bdr02.tor.packetflow.ca
3	64.34.236.121	0	0	16	0	13768	42.9833	-81.25	64.34.236.121
4	216.187.114.145	0	0	0	0	3303	40.6888	-74.0203	10ge.xe-2-0-0.tor-151f-cor-1.peer1.net
5	216.187.114.133	0	0	0	0	3303	40.6888	-74.0203	10ge.xe-0-0-0.tor-1yg-cor-1.peer1.net
6	216.187.114.141	15	16	15	16	3303	40.6888	-74.0203	oc48-po5-0.chi-eqx-dis-1.peer1.net
7	206.223.119.79	16	15	16	15	293	37.555	-122.269	ex1-g1-0.eqchil.sbcglobal.net
8	151.164.99.110	16	16	15	16	7132	38.0	-97.0	151.164.99.110
9	151.164.99.129	15	15	16	15	7132	38.0	-97.0	151.164.99.129
10	12.122.79.85	16	16	15	16	7018	38.0	-97.0	gar3.cgcil.ip.att.net
11	12.122.133.218	63	62	63	62	7018	38.0	-97.0	cr1.cgcil.ip.att.net
12	12.122.4.121	62	63	62	63	7018	38.0	-97.0	cr1.sffca.ip.att.net
13	12.123.15.110	63	62	63	62	7018	38.0	-97.0	cr83.sffca.ip.att.net
14	12.122.110.113	62	63	62	63	7018	38.0	-97.0	gar26.sffca.ip.att.net
15	12.91.92.250	62	62	63	62	7018	38.0	-97.0	12.91.92.250
16	63.197.251.33	79	63	62	63	7132	37.8033	-122.411	63.197.251.33

Table 1: TRgen output for traceroute 1859, between a home computer in Toronto, Canada and the San Francisco Art Institute, performed December 13, 2009

Where:

- **hop** = the number of the hop from the originating node (12.231.120.0)
- **IP Address** = IP address of the router or other device that corresponds to that particular

hop

- **Round trip times** are the times in milliseconds that packets take to go from the originating device to the router at that hop, and back again. The four columns correspond to four successive rounds of measuring the round trip times. They vary according to the fluctuations in traffic congestion along the route taken.
- **AS#** refers to the Autonomous System Number (ASN) of the particular network carrier for the packets. 7018 and 7132 are both ASNs of AT&T.[9]
- **Latitude and longitude** represent the geographic coordinates of the device. These figures are initially derived from GeoLite data created by MaxMind, available from http://maxmind.com/. See below for further explanation.
- **Hostname** is the network name for the device, such as found in the ARIN WHOIS Database and similar databases.[10]

<end table 1>

In this case, packets required 16 hops to go from the source computer to the destination, and took roughly 32 millisecs for the journey (i.e. half the 63 millisecs round trip time for the test packets).

From the AS numbers we can infer that the packets were handled by 4 different carriers:

AS#	Carrier
5645	TekSavvy Solutions, Inc.
13768/3303	Peer 1 Network Inc.
293	Equinix
7132/7018	AT&T WorldNet Services

With the latitude and longitude information for each hop, it is not difficult to depict this route geographically. We use Google Earth for this purpose, as it is widely available and has a relatively straightforward application programming interface (API). The IXmaps output for each route traced includes a link at the top of the table to Google Earth for this purpose. But before discussing these visual maps in more detail, we need to examine more closely the accuracy of the

[9] See AT&T Global IP Network Settlement-Free Peering Policy: http://www.corp.att.com/peering/

[10] http://ws.arin.net/whois/

geographic data.

There are many others who want to know the physical location of IP addresses, but for different reasons. To cater to this need a variety of on-line services provide location information for a given IP address or URL. One of the most prominent is Maxmind, which is the service we currently use.[11] Maxmind claims that it is "83% accurate for the US within a 25 mile radius."[12] This may be fine for Maxmind's principal target use, which is to locate the end user's devise to the accuracy of a postal code or ZIP code to aid in marketing and electronic commerce. However, it is not adequate for pinning down to specific buildings the location of core routers.

Determining the exact physical location of a particular IP address, or rather its associated router, is a notoriously difficult task (Dodge and Kitchen 2002). This is especially challenging in the case of internet core facilities, as it relies on ISPs regularly reporting publically precise, accurate and up to date location information about their routers. There is little incentive the carriers to do this, while incurring various risks.

[11] Some of the other similar geo-location services are:

Quova: http://www.quova.com/

IP2Location: http://www.ip2location.com/

GeoBytes: http://www.geobytes.com/ipLocator.htm

InfoSniper: http://www.infosniper.net/index.php?lang=1

IPGlobalPosition: http://www.ipglobalposition.com

[12] http://www.maxmind.com/app/faq#accurate

In particular, we have found so far that most of the IP addresses associated with internet core routers are given generic locations or associated with corporate head offices rather than the actual switching centers. We can see this in the example above. Maxmind reports that almost every IP address associated with AT&T (i.e. hops 8 to 16) has a lat/long of 38.0 -97.0. The rounding of these figures to a full degree, and the corresponding lack of trailing decimal digits, provides an obvious clue that these do not correspond to actual physical locations. In this case 38, -97 corresponds to a vacant corn field in Kansas near the geographic centre of the continental US.[13] Furthermore, three of the apparently more precise locations mentioned above represent the official business addresses of the carriers, as listed in the ARIN WhoIs database, but are no more accurate. Table 2 includes examples of these erroneous latitude and longitude assignments.

The only location we can have any confidence in is the very last, as 37.8033, -122.411 is a few blocks from the known location of the San Francisco Art Institute (800 Chestnut Street) and corresponds to the geographic center of the Institute's zipcode (94133)

[13] The official Geographical Center of the United States is Latitude 39 degrees 50 minutes Longitude 98 degrees 35 minutes. See: http://www.kansastravel.org/geographicalcenter.htm

<begin Table 2>

Hop	Latitude	Longitude	Carrier	Remarks
1	42.4	-82.1833	Teksavvy	these coordinates correspond to the small town of Chatham ON, Teksavvy's headquarters; the router itself is known to be located in downtown Toronto
4-6	40.6888	-74.0203	Peer 1	these coordinates correspond to New York City, Peer 1's business address, whereas the routers appear to be in Toronto and Chicago
7	37.555	-122.269	Equinix	these coordinates correspond to Foster City CA, whereas this router appears to be in Chicago
8-15	37.0	-97.0	AT&T	these coordinates correspond to the centre of the U.S., whereas the routers appear to be in Chicago and San Francisco

Table 2: Locational anomalies in MaxMind's GeoLite database for traceroute 1859.

<end table 2>

It is clear from this analysis that Maxmind location data does not provide an accurate basis for mapping the routes packets take within the internet core. Unfortunately, the other geo-location services do no better. This means that we cannot rely on conventional approaches for mapping internet backbone routers and associated IP addresses. We need to supplement the generally available and adequately reliable IP location data for edge routers with additional location data on the core routers gathered from other sources.

Fortunately for us, unlike their reticence about making public the location of particular IP addresses, carriers are relatively forthcoming about the hostnames that are associated with IP addresses. We can see this in the example above as most hops have apparently meaningful hostnames. This may be because these names are helpful for network management and diagnostics.

Do these hostnames provide sufficient information to link the associated IP addresses with specific buildings? Let's take a look, focusing on AT&T.

There are 155 IP addresses in the IXmaps database associated with ATT, that is, having an AS number of 7018. Most have elaborate hostnames s containing clues about the cities they are located in. Here is a sampling of the ATT host names we found that are suggestive of their locations:

```
cr1.attga.ip.att.net - Atlanta GA
cr2.wswdc.ip.att.net - Washington DC
cr2.dlstx.ip.att.net - Dallas TX
cr2.dvmco.ip.att.net - Denver CO
cr2.la2ca.ip.att.net – Los Angeles CA
cr2.sffca.ip.att.net - San Francisco CA
cr2.st6wa.ip.att.net - Seattle WA
```

There were several minor variations on the prefixes in these URLs. In addition to the ‘`cr1`’ and ‘`cr2`’ prefixes seen here, we also found similar AT&T routers with the prefix ‘`gar`’ followed by a one or two digit number (e.g. ‘`gar26`’). We surmise that ‘`cr`’ corresponds to ‘core router’, or a router that mainly exchanges traffic with other relatively distant core routers, and ‘`gar`’ corresponds to ‘gateway router’, or a router that serves as a local gateway to the internet core, or as an exchange point between networks in the core.

We were principally interested in AT&T’s San Francisco operations, as this is where Mark Klein identified AT&T’s facilities at 611 Folsom Street as the location of the splitter room he helped install. Here are all the AT&T hostnames in the IXmaps database that contain the string ‘`sffca`’:

```
12.122.4.121    |  7018 |       38 |       -97 | cr1.sffca.ip.att.net
12.122.3.121    |  7018 |       38 |       -97 | cr1.sffca.ip.att.net
12.122.31.134   |  7018 |       38 |       -97 | cr2.sffca.ip.att.net
12.122.110.113  |  7018 |       38 |       -97 | gar26.sffca.ip.att.net
12.123.15.110   |  7018 |       38 |       -97 | cr83.sffca.ip.att.net
12.123.15.250   |  7018 |       38 |       -97 | cr84.sffca.ip.att.net
```

Each of these IP addresses show up in our database repeatedly, each time near the end of the traceroute of a destination within the SF area. This further confirms that these IP addresses and hostnames refer to AT&T’s principal San Francisco routers.

Since 611 Folsom St is AT&T’s main internet peering and exchange point in San Francisco, there is good reason to believe that these 6 IP address correspond to that location. Hence trace routes that contain any of these 6 IP addresses are very likely to pass through 611

Folsom St and thus to be subject to NSA surveillance.[14]

On this basis, we re-assigned the latitude and longitude of any hostname including the string “sffca” to 37.7852, -122.397, the location of 611 Folsom Street.

With this explanation in mind, and recognizing the limitations of the geo-location process so far, let’s turn now to the second major part of the IXMaps program, the cartographic visualization of individual traceroutes. This visualization relies in part on another database of “interesting” properties of the real estate through which the packet passes. Now in its prototype stage, this database consists information regarding about 50 carrier hotels. It includes their latitude and longitude coordinates, their street addresses, the carriers known to use the facility, and in some cases ownership information and photos. We have developed KML files to integrate these data with the traceroute data and to display them using Google Earth. Figures 1 through 3 show several screen shots of this program.

Clicking on the “Google Maps” link in the initial table produced by TRgen produces the image shown in Figure 1. The packets start in Toronto, and end in San Francisco. Zooming in on the destination produces the image in Figure 2. The small squares are router locations. In this case the red square corresponds to 611 Folsom Street. Clicking on this square produces the pop-up image shown in Figure 3, with a photograph of the building and other details about the carrier hotel operations there.

[14] Note the ‘second ‘f’ in ‘sffca’ is also suggestive of Folsom Street. It is quite possible that there are other IP addresses at Folsom St, but without the conveniently readable hostnames.

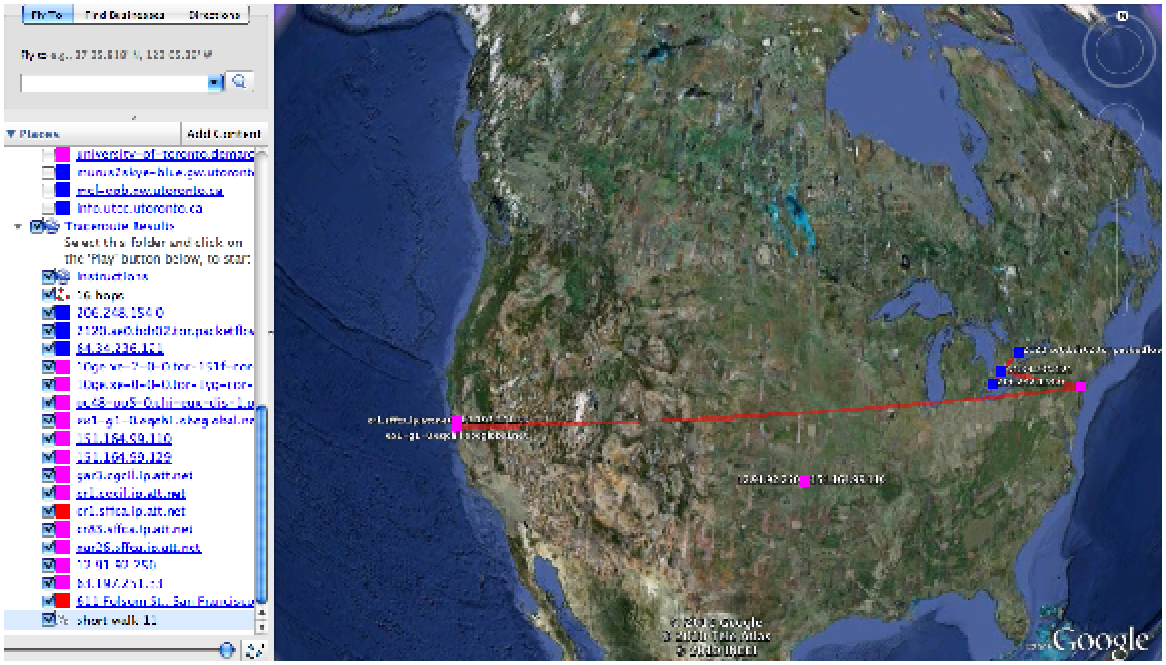


Figure 1: IXmaps rendering of traceroute #1859 with Google Earth (screenshot)

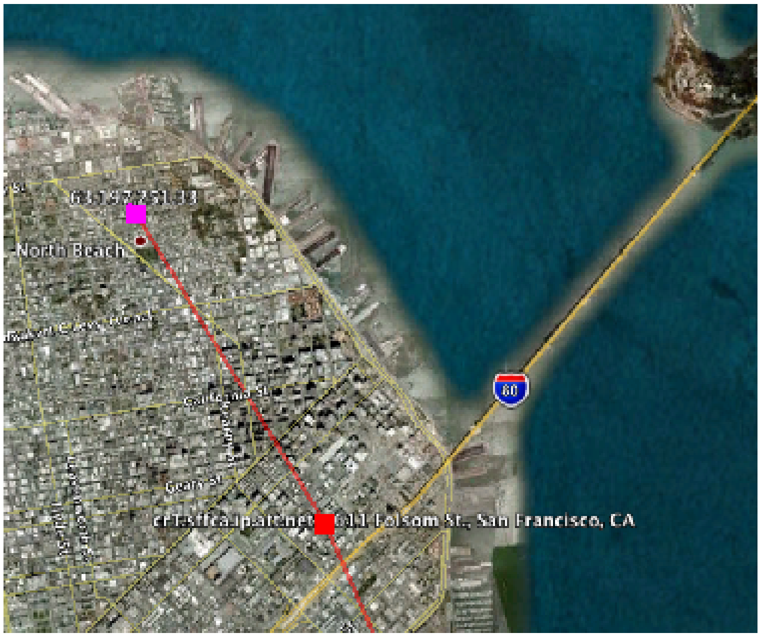
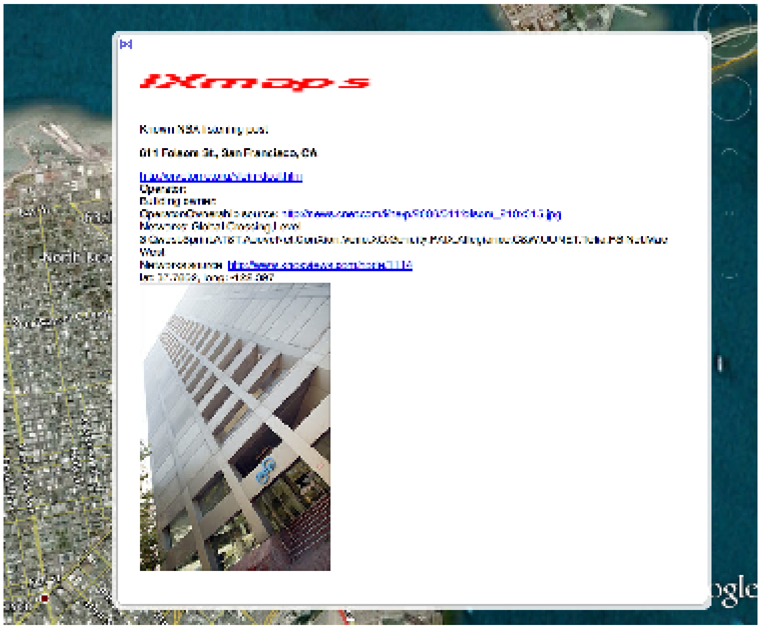


Figure 2: IXmaps rendering of traceroute #1859 with Google Earth – San Francisco business district zoom (screenshot)



IXmaps

Known NSA listening post

611 Folsom St., San Francisco, CA

[illegible]
Operator:
Building owner:
Operator/Ownership source: [illegible].jpg
Members: Global Crossing Level
3 Qwest Sprint AT&T [illegible]
[illegible]
Networks source: [illegible]
lat: 37.7[illegible], long: -122.397

Figure 3: IXmaps rendering of traceroute #1859 with Google Earth – San Francisco business district zoom, with pop-up view of 611 Folsom Street site (screenshot)

DISCUSSION

IXmaps is very much a work in progress. What we have been able to demonstrate so far is a proof of concept – that it is possible to show vividly some aspects of what is usually out of view and obscured by regimes of secrecy and technical inscrutability.

Our plans for the further development of the IXmaps software include:

- geo-locating more of the high traffic core routers so that the routes are mapped more accurately.
- incorporating a "confidence" marker in the TRgen database and referring to that marker in the KML programs. This marker will stand for the algorithm we used to infer geo-location, and will permit interested users to review that algorithm and judge for themselves its reliability.
- incorporating information on more of the carrier hotels, especially those associated with carriers that complied with NSA surveillance requests
- extending the type of information associated with carrier hotels, eg. energy consumption/efficiency, corporation ownership
- increasing the graphic sophistication of the maps, eg. by using different colors to

display the parts of the route carried by different carriers, or by visually dithering nodes depending on the reliability of the locational information.

These steps will contribute to dispelling the myth of the internet core as being like a "cloud", a place-less, people-less ethereal space where our transactions get seamlessly and unproblematically routed to just where they should without us having to be concerned about how. In particular, we hope in these ways to make the surveillance in everyday life more visible, and hence more democratically accountable.

ACKNOWLEDGMENTS

We appreciate contributions by Steve Harvey for the software programming that makes IXmaps function, and by Yannet Lathrop for preparing the Appendix. This research was supported by an Image, Text, Sound and Technology (ITST) grant of the Social Sciences and Humanities Research Council (SSHRC).

For more on IXmaps, see http://iprp.ischool.utoronto.ca/node/36. The TRgen program and the traceroute database is available at http://www.ixmaps.ca.

REFERENCES

Bamford, J. (2008). *The shadow factory*. New York: Random House.

Dodge. M. and Kitchen, R. (2002) "New Cartographies to Chart Cyberspace" *Geoinformatics* (April/May): 1.

Savageau, John. (n.d.) Net Neutrality and the Carrier Hotel. Ezine Articles website. Article Source: http://ezinearticles.com/?Net-Neutrality-and-the-Carrier-Hotel&id=319274

Young. R. (Producer). (2007, May 16). *Spying on the home front*. [Television broadcast]. Boston: wgbh educational foundation. Transcript Retrieved Sept 1, 2008, from: http://www.pbs.org/wgbh/pages/frontline/homefront/interviews/klein.html

APPENDIX

Report on NSA court cases concerning alleged NSA warrantless surveillance programs

prepared by Yannet Lathrop

AT&T

In early 2006, Mark Klein, a former AT&T technician, revealed to the media that his former employer had allowed the National Security Agency (NSA) to install splitters in the telecom's 611 Folsom Street, San Francisco, California location.[15] Soon after this revelation, more substantive investigations followed, and AT&T found itself the defendant in a lawsuit (*Hepting v. AT&T*) launched by the Electronic Frontier Foundation in May 2006 on behalf on affected AT&T customers.

In *Hepting v. AT&T,* the plaintiffs allege that AT&T provided and (as of the date of the lawsuit) continues to provide direct access of "all or a substantial number of the communication transmitted through its key domestic telecommunications facilities, including direct access to streams of domestic, international and foreign telephone and Internet communication" to the U.S. Government.[16] The plaintiffs further allege that AT&T installed and used, or assisted the government with the installation and use, of "interception devices and pen registers and/or trap and trace devices on or in a number of its key telecommunications facilities;" and that AT&T granted, and continues to grant, the government with direct access to "its databases of stored telephone and Internet records," including detailed call records.[17]

The plaintiffs claimed that, in cooperating with the NSA's extralegal requests, AT&T was acting as an instrument or agent of the state, thereby violating the plaintiffs' First and Fourth Amendment rights under the Constitution of the United States—which protect free speech,

[15] Richtel, M. & Belson K. 2006. "U.S. focused on obtaining long-distance phone data, company officials indicate." *The New York Times* (18 May); http://www.nytimes.com/2006/05/18/us/18call.html.
Electronic Frontier Foundation. (n.d.). *AT&T's Role in Dragnet Surveillance of Millions of Its Customers: Internet Spying in San Francisco*; http://www.eff.org/cases/hepting.

[16] *Hepting v. AT&T*, No. C-06-0672-JCS (U.S. District Court, Northern District of California. February 22, 2006). Par. 42.

[17] Ibid., Par. 43, 51, 54-64.

provides individuals with a reasonable expectation of privacy and guard against unreasonable searches and seizures, respectively.[18]

VERIZON/MCI

According to the *Master Consolidated Complaint Against MCI Defendants and Verizon Defendants* filed with the U.S. District Court, Northern District of California (San Francisco Division), filed by Elisabeth J. Cabraser et al., on behalf of Verizon and MCI customers, MCI was among the telecommunications companies that turned over call records and granted the government access to their systems without warrants of court orders, based solely on "oral requests from senior government officials."[19]

This document also alleges that, "Defendants have intercepted and continue to provide the government with direct access to all or a substantial number of the communications transmitted through their key domestic telecommunications facilities, including direct access to streams of domestic, international, and foreign telephone and electronic communications."[20]

As well, this document alleges that Verizon and MCI have either allowed or assisted the government with the installation of "interception devices and pen registers and/or trap and trace devices" on their domestic telecommunications facilities, and that they continue to do so as of the date of the document.[21]

BELLSOUTH

According to the *Master Consolidated Complaint Against Defendant "BellSouth" For Damages, Declaratory and Equitable Relief*, filed with the U.S. District Court, Northern District of California (San Francisco Division), BellSouth began supplying telephone call and internet records to the federal government at some time on or after February 1, 2001, and that it continued to do so as of the date of the complaint.[22]

[18] Ibid., Par. 85.

[19] *Master Consolidated Complaint Against MCI Defendants and Verizon Defendants*, No. 06-1791 VRW (U.S. District Court, Northern District of California, San Francisco Division, January 16, 2007). Par. 148, 158. (See also Par. 169).

[20] Ibid., Par. 168. (See also Par. 171 and 176).

[21] Ibid., Par. 173.

[22] *Master Consolidated Complaint Against Defendant "BellSouth" For Damages, Declaratory*

It is also alleged in this document that "BellSouth has intercepted and continue to provide the government with direct access to all or a substantial number of the communications transmitted through its key domestic telecommunications facilities, including direct access to streams of domestic, international, and foreign telephone and Internet communications."[23]

As well, this document alleges that BellSouth has either allowed or assisted the government with the installation of "interception devices and pen registers and/or trap and trace devices" on its domestic telecommunications facilities, and that it continues to do so as of the date of the document.[24]

CINGULAR

According to the *Fist Amended Master Consolidated Complaint Against Defendants AT&T Mobility LLC (f/k/a Cingular Wireless LLC)..."* filed with the U.S. District Court, Northern District of California (San Francisco Division), since October 2001, Cingular has "disclosed and/or divulged the 'call-detail records' of all or substantially all of their customers including Plaintiffs to the NSA."[25]

The document also alleges that Cingular "intercepted and continue to provide the government with direct access to all or a substantial number of the communications transmitted through its key domestic telecommunications facilities, including direct access to streams of domestic, international, and foreign telephone and Internet communications"[26]

Finally, this document also alleges that Cingular has either allowed or assisted the government with the installation of "interception devices and pen registers and/or trap and trace

and Equitable Relief, No. 06-1791 VRW (U.S. District Court, Northern District of California, San Francisco Division, January 16, 2007). Par. 37, 68 and 70.

[23] Ibid., Par. 67.

[24] Ibid., Par. 72. (See also Par. 75).

[25] *First Amended Master Consolidated Complaint Against Defendants AT&T Mobility LLC (f/k/a Cingular Wireless LLC), Cingular Wireless Corp., and New Cingular Wireless Services, Inc. For Damages, Declaratory and Equitable Relief,* No. 06-1791 VRW (U.S. District Court, Northern District of California, San Francisco Division, July 03, 2008). Par. 57.

[26] Ibid., Par. 56.

devices" on its domestic telecommunications facilities, and that it continues to do so as of the date of the document.[27]

SPRINT

According to the *Master Consolidated Complaint Against Defendants Sprint Nextel Corporation...For Damages, Declaratory and Equitable Relief*, filed with the U.S. District Court, Northern District of California (San Francisco Division), since October 2001, Sprint has "disclosed and/or divulged the 'call-detail records' of all or substantially all of their customers including Plaintiffs to the NSA."[28]

This document also alleges that Sprint has either allowed or assisted the government with the installation of "interception devices and pen registers and/or trap and trace devices" on its domestic telecommunications facilities, and that it continues to do so as of the date of the document.[29]

The document also alleges that Sprint has "knowingly authorized, and continue to knowingly authorize, NSA and affiliated governmental agencies to directly access through the installed devices all wireless telephone communications transmitted through the Defendants' domestic telecommunications infrastructure and facilities."[30]

QWEST

Unlike BellSouth, AT&T, Verizon/MCI, Cingular and Sprint, the *Wall Street Journal* reported that Qwest did not comply with the NSA's request to turn in customers' telephone records.[31] The *Denver Post* reports that this request was made in February 2001, well before the

[27] Ibid., Par. 61. (See also Par. 64).

[28] *Master Consolidated Complaint Against Defendants Sprint Nextel Corporation, Sprint Communications Co. Ltd Partnership, Nextel Communications, Inc., Embarq Corporation, UCOM, Inc., U.S. Telcom, Inc., and Does 1-100 For Damages, Declaratory and Equitable Relief,* No. 06-1791 VRW (U.S. District Court, Northern District of California, San Francisco Division, January 16, 2007). Par. 48.

[29] Ibid., Par. 52.

[30] Ibid., Par. 55.

[31] Young, S. & Searcey, D. (13 May 2006). Nacchio confirms rejecting request from NSA –

attacks of September 11, 2001.[32] Qwest refusal has been documented in the *Master Consolidated Complaint Against MCI Defendants and Verizon Defendants*, Paragraph 153. (See "Verizon/MCI" below for citation).

In addition to requests for phone records, Qwest was also approached by unnamed "clandestine agencies" about allowing the latter the use of Qwest's "fiber-optic communications network for government purposes."[33] On this issue, the *Pittsburgh Post-Gazette* reported that in early 2001, the NSA requested access to Qwest's "most localized communications switches, which primarily carry domestic calls," and proposed that access be obtained through the installation and use of monitoring equipment on the telecom's "Class 5" switching facilities [34] Qwest, which was worried that such access would "have permitted neighborhood-by-neighborhood surveillance of phone traffic without a court order," refused to comply with this request.[35]

Qwest ex-chief refused access to records; case may get a new twist. *The Wall Street Journal*, A3.

[32] Young, A. (21 October 2007). Nacchio affects spy probe His court filings point to government surveillance months before 9/11Claims in the ex- Qwest CEO's case could shift the debate over the federal pursuit of warrantless wiretapping. *Denver Post*, K1.

[33] Ibid., (under heading "Ties to Secret Agencies.")

[34] Lichtblau, E. (16 December 2007). Wide monitoring fuels plan to protect phone industry. *Pittsburgh Post-Gazette*, A11.

[35] Ibid.