

Privacy and National Security in the age of the Internet

Breen Agnew | Jack Morrison

DATA DEMOCRACY?

Discussion

1. Net Neutrality
2. Deep Packet Inspection
3. Short Video
4. Data and National Security
5. Case Study: AT&T and NSA

Network Neutrality

Definition: Net Neutrality is the principle that the Internet should be kept open and free from interference or restrictions from service providers. That is, certain users or applications should not be favored over another.



Network Neutrality

- Sources of Net Neutrality Infringement:
 - Content Providers issuing licensing agreements to ISP's
 - ISP's and Govt's with DPI technology

START WATCHING NOW!

Your provider doesn't offer ESPN360.com, but those listed below do!
Click a provider to see how you can make the switch today!

AT&T Yahoo! **GO**

Demand live sports online 24/7!

Tell The Sequoias Apartments you want ESPN360.com.

First Name: Last Name:

Email: Birthdate: (MM/DD/YYYY)

Comments:

I'd like to receive occasional updates, special offers, and other information from ESPN regarding my favorite teams, favorite sports and other areas of interest.

I'd like to receive occasional updates, special offers, and other information from The Walt Disney Company family of businesses.

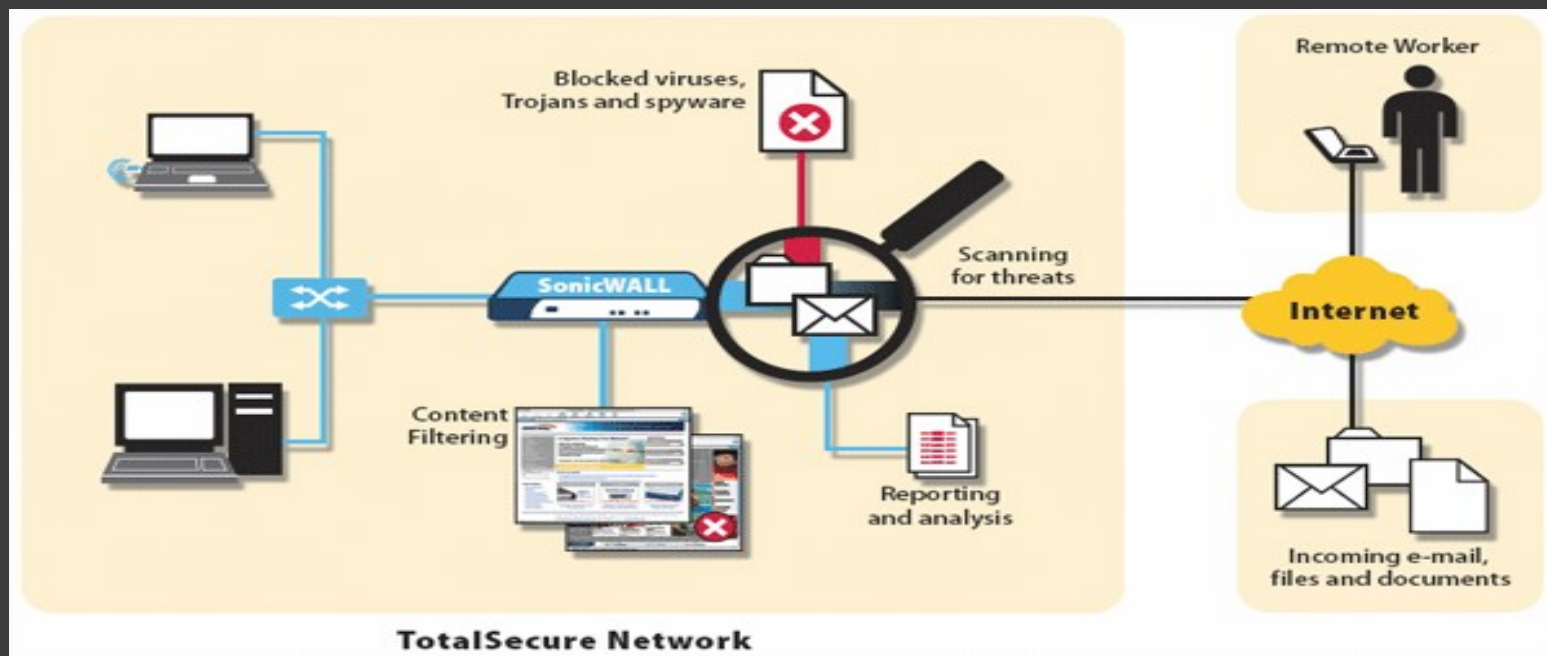
I'd like to receive occasional updates, special offers, and other information from carefully selected third parties regarding my favorite teams, favorite sports and other areas of interest.

You may receive the above communications by email, postal mail, and other means. **SEND**

Deep Packet Inspection

Definition: Firewall technology that combines IDS, IPS, and Stateful Firewall.

- Capabilities: Security + Advanced Packet Inspection



Deep Packet Inspection

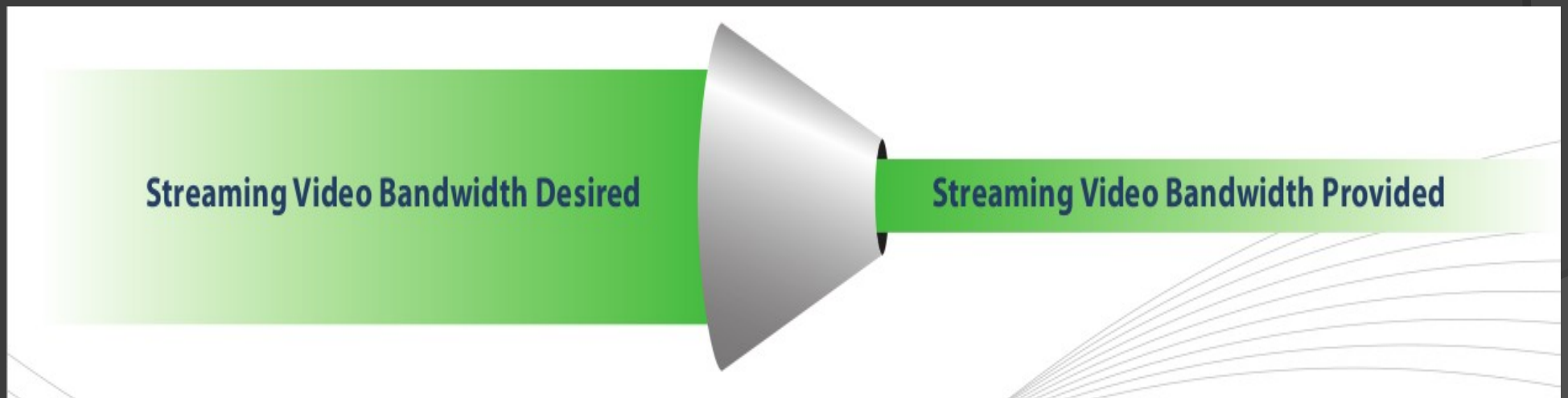
- Typical DPI Vendor Solutions:
 - Traffic Management
 - Content Filtering
 - Parental Controls
 - Interception



Deep Packet Inspection

Content Filtering:

- Manage and control content on the network in a personalized, Per-User/Subscriber basis.



Deep Packet Inspection

Parental Controls:

- Revenue Generation

Interception:

- Wiretapping



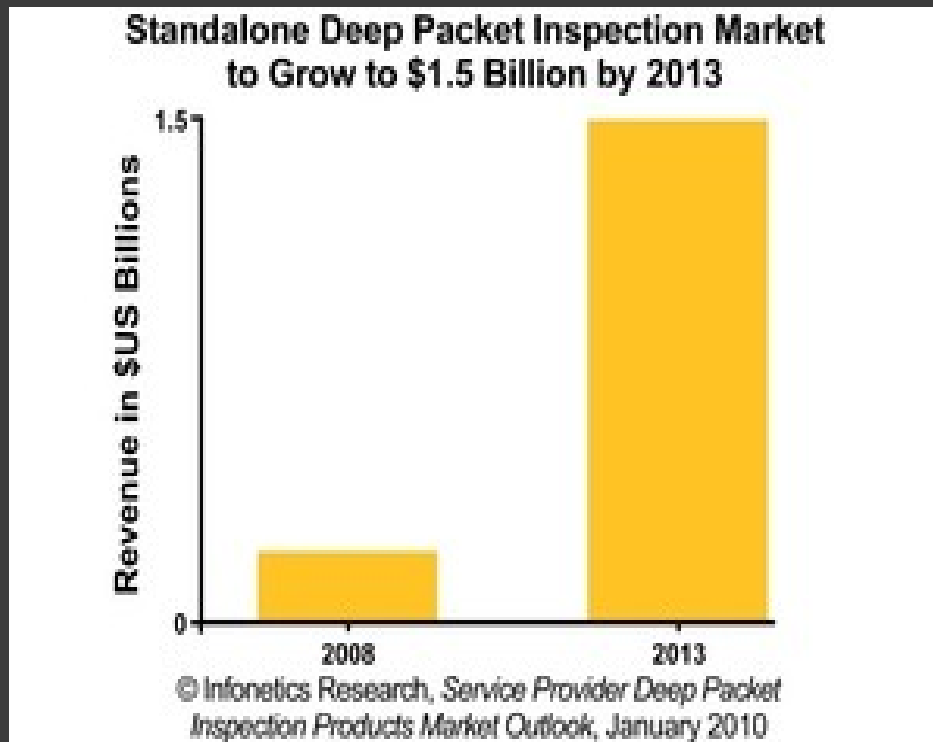
Sources:

<http://www.att.com>

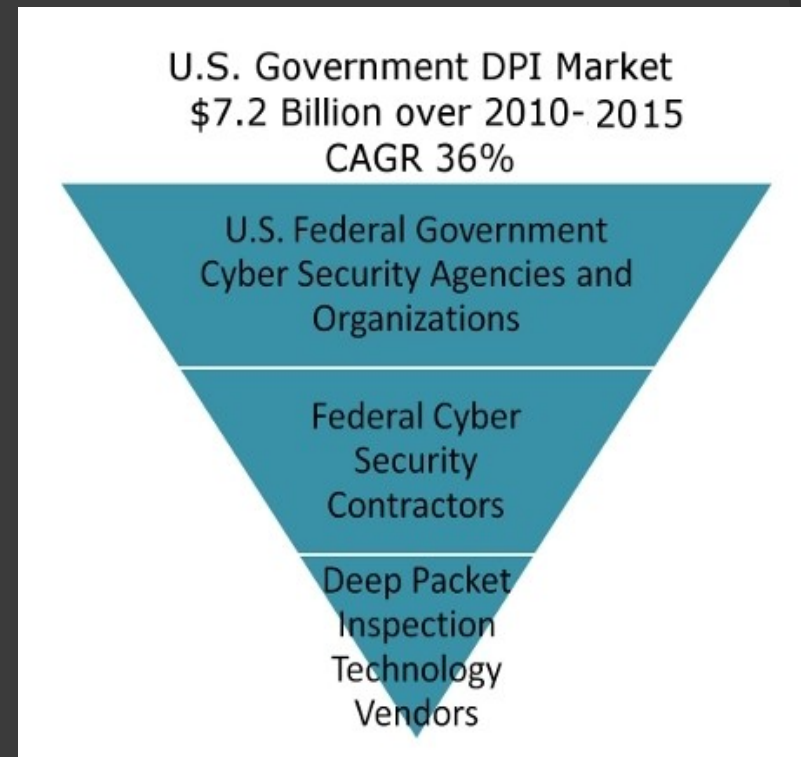
<http://easytechsource.com/security/ComputerSecurity.jpg>

Deep Packet Inspection Market Projections

Global Market



U.S Gov't Market



Sources:

<http://www.marketresearchmedia.com/2010/02/17/deep-packet-inspectionmarket/>

<http://www.cbc.ca/technology/story/2009/07/02/f-net-neutrality-faq.html>

Part 2: Nat'l Security and Spying

- National Security and Information Assurance Policies
- Pre and Post 9/11 Era in Information security and intelligence
- What do these agencies do?
- What's the big deal?

Short Clip – The NSA and AT&T

<http://www.pbs.org/wgbh/pages/frontline/homefront/>

~5:08

The NSA and CSE



□ NSA - National Security Agency

- November 4th, 1952
- Mission: "...delivering responsive, reliable, effective, and expert Signals Intelligence and Information Assurance products and services, and enables Network Warfare operations..."

□ CSE - Communications Security Establishment

- To provide and protect information of national interest through leading-edge technology, in synergy with our partners.
- Canadian government's foreign intelligence and national cryptologic agency. Administered under the Department of National Defence (DND)
 - Formed 1946
 - Absolutely Forbidden to collect intelligence on Canadian Citizens
 - You've probably driven past it...
 - Sir Leonard Tilley Building at 719 Heron Rd.

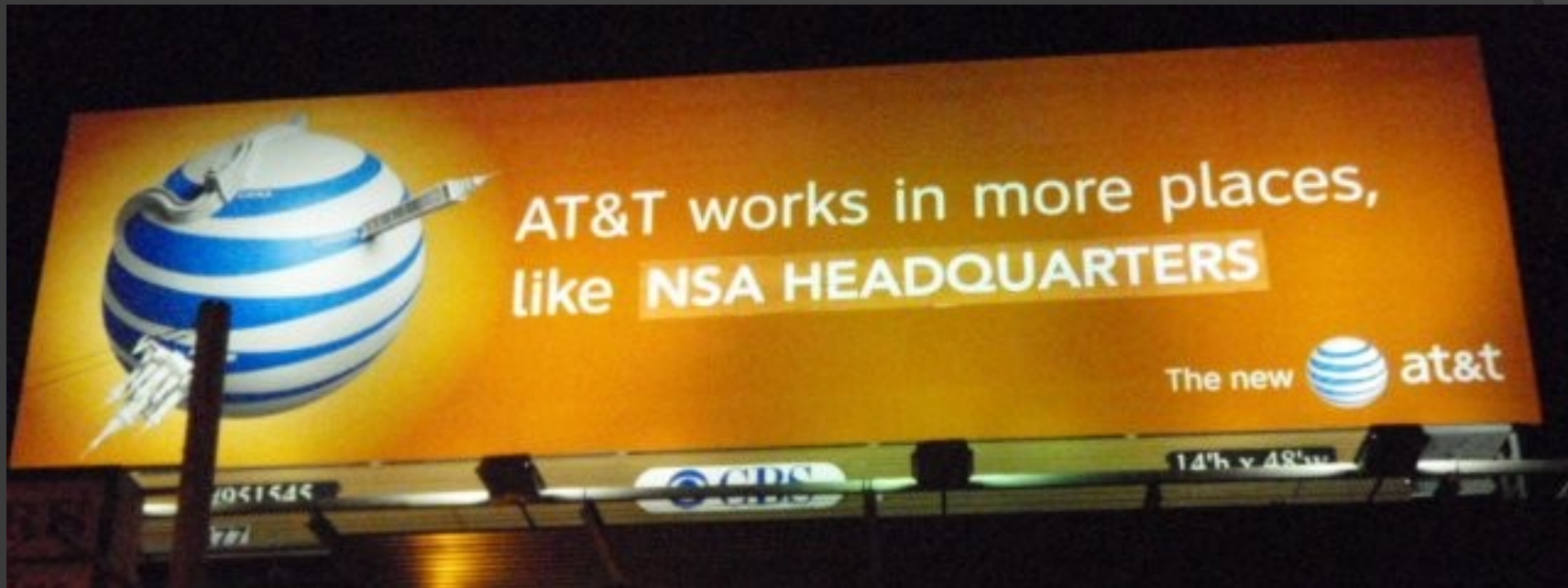
Canada's National Security Policy

- provide foreign intelligence to the Government of Canada according to Cabinet-approved priorities
- strengthen Canada's capacity for secure communications
- protect its vital electronic information and information systems
- "CSEC is forbidden, by law, to intercept domestic communications. When intercepting communications between a domestic and foreign source, the domestic communications are destroyed or otherwise ignored..."

The NSA and SIGINT - Post 9/11

- ▣ Began to engage in unlawful surveillance under the Bush administration; Warrant-less surveillance or Terrorist Surveillance program
- ▣ SIGINT - Signals Intelligence
- ▣ FISA Court (Foreign Intelligence Surveillance Act)
 - "Foreign Power; Agents of a foreign power"
 - "knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;"
- ▣ Domestic Traffic Interception

AT&T in trouble with the EFF



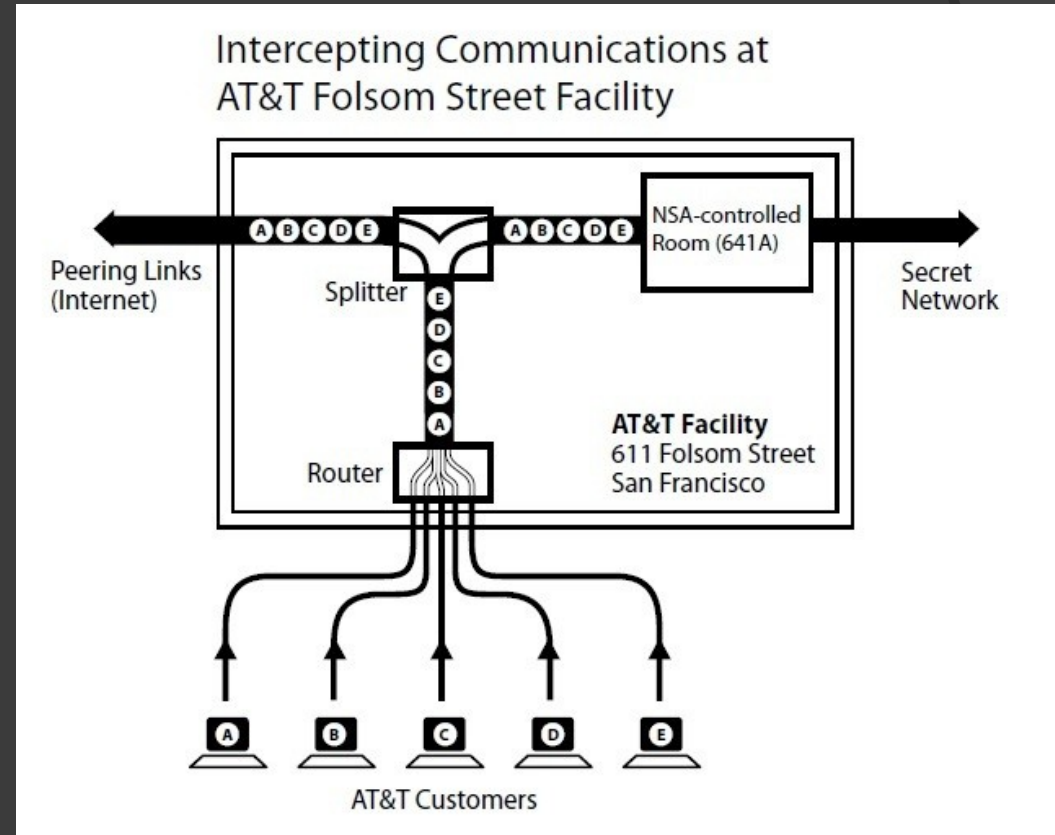
- AT&T ISP and Telecom provider for millions
- Has lines running through Mae East and Mae West
 - OC48 (Regional ISP Backbone @ 2488.32 Mbit/s)
- EFF = Electronic Frontier Foundation
 - Class Action Lawsuit vs. AT&T (Hepting v. AT&T)

Photo: <http://billboardliberation.com/HQ.html>

Sources: <http://info.ipinc.net/support/faqs/mae.html>; <http://www.eff.org/files/nsa/att.pdf>

A spy's tools

- AT&T IXP feeds into WorldNet IXP
- Fiber Splitter
 - Beam Splitter; major process
 - Exact duplicates of light particles
- Old days - Copper Wire was easy
- Narus STA 6400 - DPI
 - Carrier Grade
 - Semantic Network Traffic Analyzer



Mark Klein and Room 641a

1 I, Mark Klein, declare under penalty of perjury that the following is true and correct:
2 I. I am submitting this Declaration in support of Plaintiffs' Motion for a
3 Preliminary Injunction. I have personal knowledge of the facts stated herein, unless stated
4 on information and belief, and if called upon to testify to those facts I could and would
5 competently do so.

- AT&T Whistle Blower
 - Network Technician
 - Noticed documents and router at AT&T facility
 - Expert testimony
- Brought Room 641a to public attention
 - Viewed splitter box and Narus STA 6400
 - Provided expert testimony and supporting documents
 - "Dec. 10, 2002, [manual](#) titled "Study Group 3, LGX/Splitter Wiring, San Francisco," a Jan. 13, 2003, [document](#) titled "SIMS, Splitter Cut-In and Test Procedure" and [a second](#) "Cut-In and Test Procedure" dated Jan. 24, 2003."

Today's Reality

- ▣ Other Splitter Cabinets at AT&T facilities
- ▣ Many different provider hubs and IXC's
- ▣ Drowning in Data
 - Cray Super computers and beyond
- ▣ ECHELON
 - *AUSCANZUKUS*
- ▣ TIA (Total Information Awareness)

Questions? Comments?

- <http://www.wired.com/science/discoveries/news/2006/05/70944>
- <http://en.wikipedia.org/wiki/Narus>
- <http://www.wired.com/science/discoveries/news/2006/05/70914>
- <http://www.eff.org/files/nsa/att.pdf>
- <http://en.wikipedia.org/wiki/MAE-East>
- <http://info.ipinc.net/support/faqs/mae.html>
- Bamford, James. *The Shadow Factory: the Ultra-secret NSA from 9/11 to the Eavesdropping on America*. New York: Doubleday, 2008. Print.
- Christensen, Chris. "Review of *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America* by James Bamford" *Cryptologia* 33.4 (2009). 29 Mar. 2010
< <http://www.informaworld.com/10.1080/01611190903115150> >
- www.ibm.com
- www.juniper.net
- www.narus.com