Preparing for the Future Internet

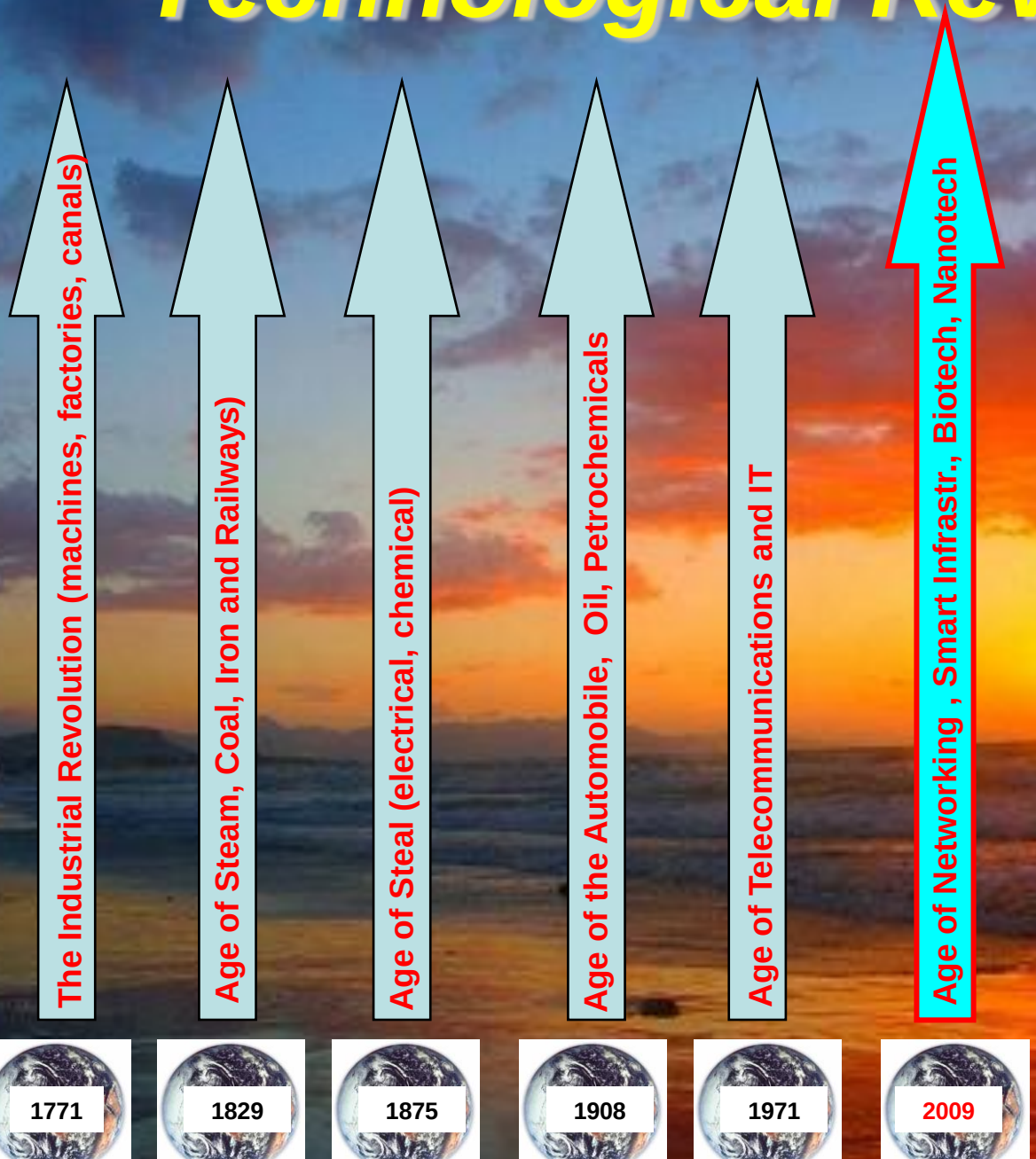
Europe in Action

Dr. Joao Schwarz Da Silva
European Commission

ENISA Summer School
Crete, 14-17 September 2009


How were the successive technology revolutions unleashed?
By widening demand and stretching the reach of the infrastructures

Technological Revolutions



Each Revolution transforms the economy and drives a great surge of development and shapes innovation for 50 years or more

Each Revolution reshapes the opportunity space and the ways of living and working

At the beginning of a new Era

- Mature industries are close to technology exhaustion, their innovation drive is weak
- Old economies stagnate, new technologies are incipient
- Need to select the new engines of growth
- Moving from laissez faire to the active comeback of the state
- Shifting from supply-push to demand-pull in investment and innovation
- Moving from individual focus to collective interests
- Old industries and markets are rejuvenated
- Making the best out of our technological potential

Drivers

Rising costs of energy, transport, health

Huge inefficiencies in energy and transport and health related processes

Growing environmental threats

Growing security threats

Untapped potential of ICT as smart infrastructure enablers

Opportunities

Energy distribution and management

Transport, mobility, architecture, urban planning

Production, waste disposal, recycling

Health, well being, third age

Sports, leisure, culture

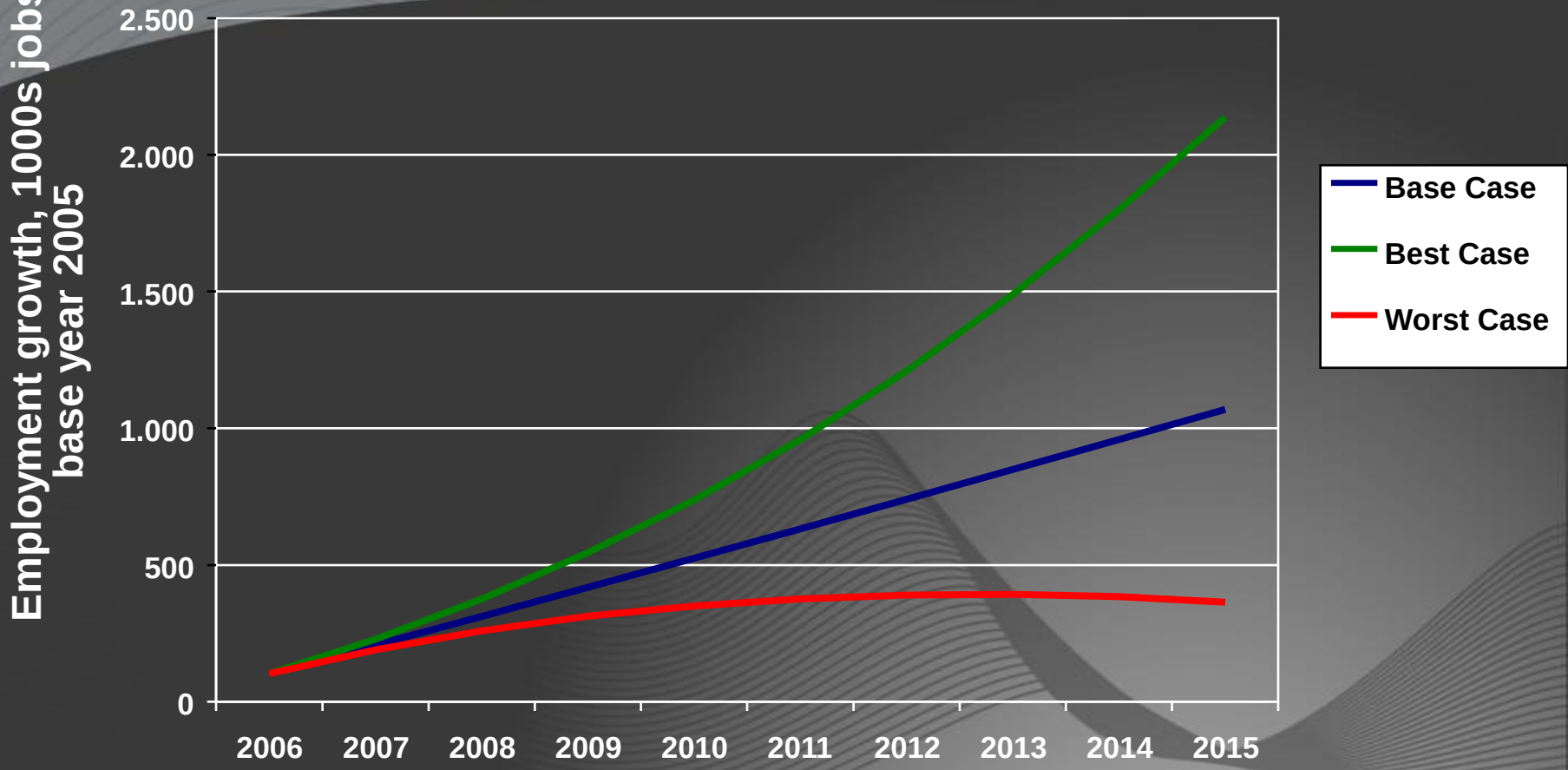
A Profound social and economic business transformation

- We are now all connected: technically , socially and economically
- The world is becoming smarter: systems, processes, service delivery
- The world is becoming instrumented, interconnected, intelligent
- Turning data into intelligence
- Analytics market segment exceed ERP market segment
- Traffic jams costs europe 135 B€ annually
- 40 to 70% of all electrical energy is lost because of inefficient grids
- 1 billion lines of code in an Airbus
- 100 million lines of code in a vehicle

The Job Creation Potential of Europe's Digital Economy

Impact of broadband on the economy

Broadband-related employment growth (EU27, 2006-2015, cumulative)



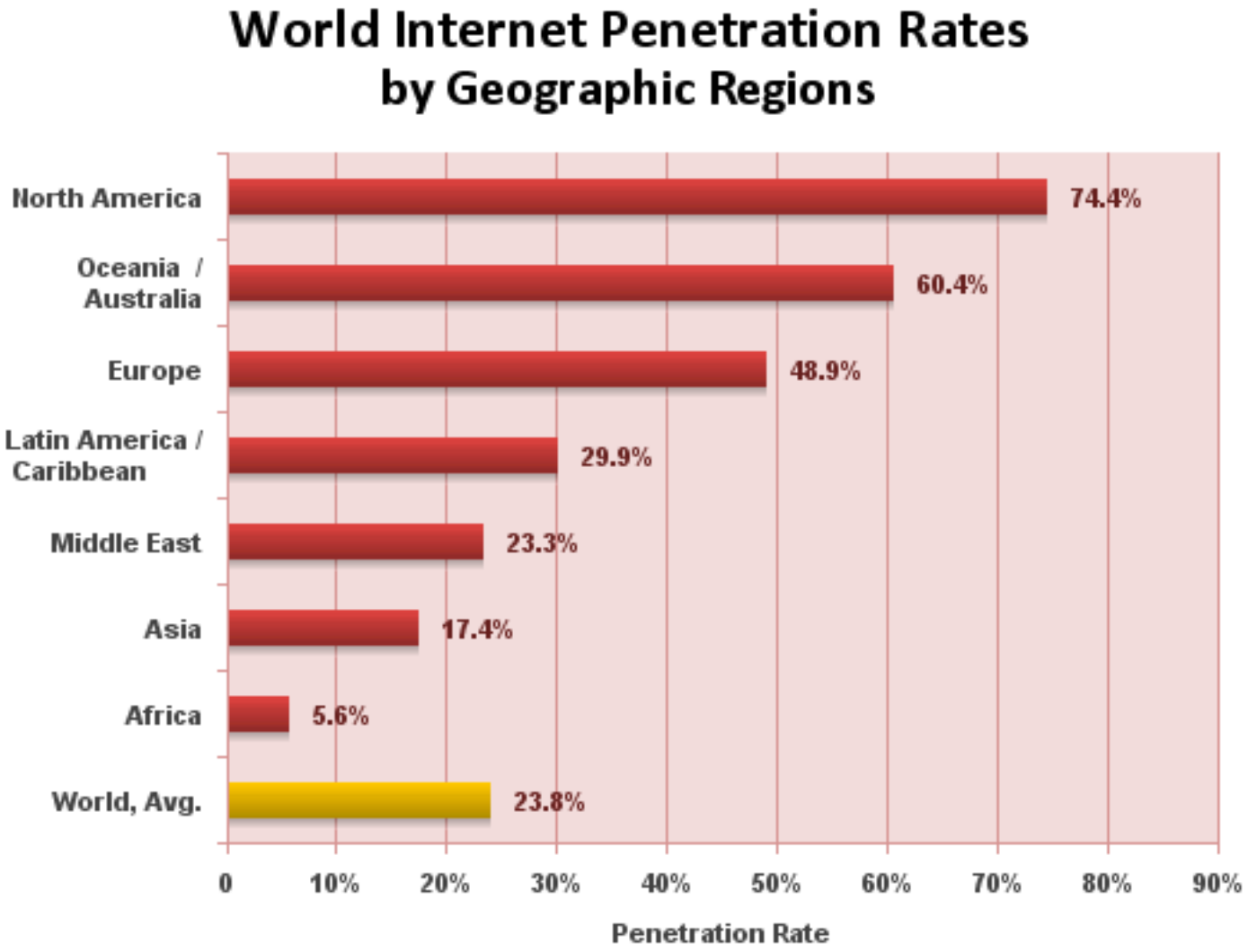
INTERNET USAGE STATISTICS
The Internet Big Picture
World Internet Users and Population Stats

WORLD INTERNET USAGE AND POPULATION STATISTICS

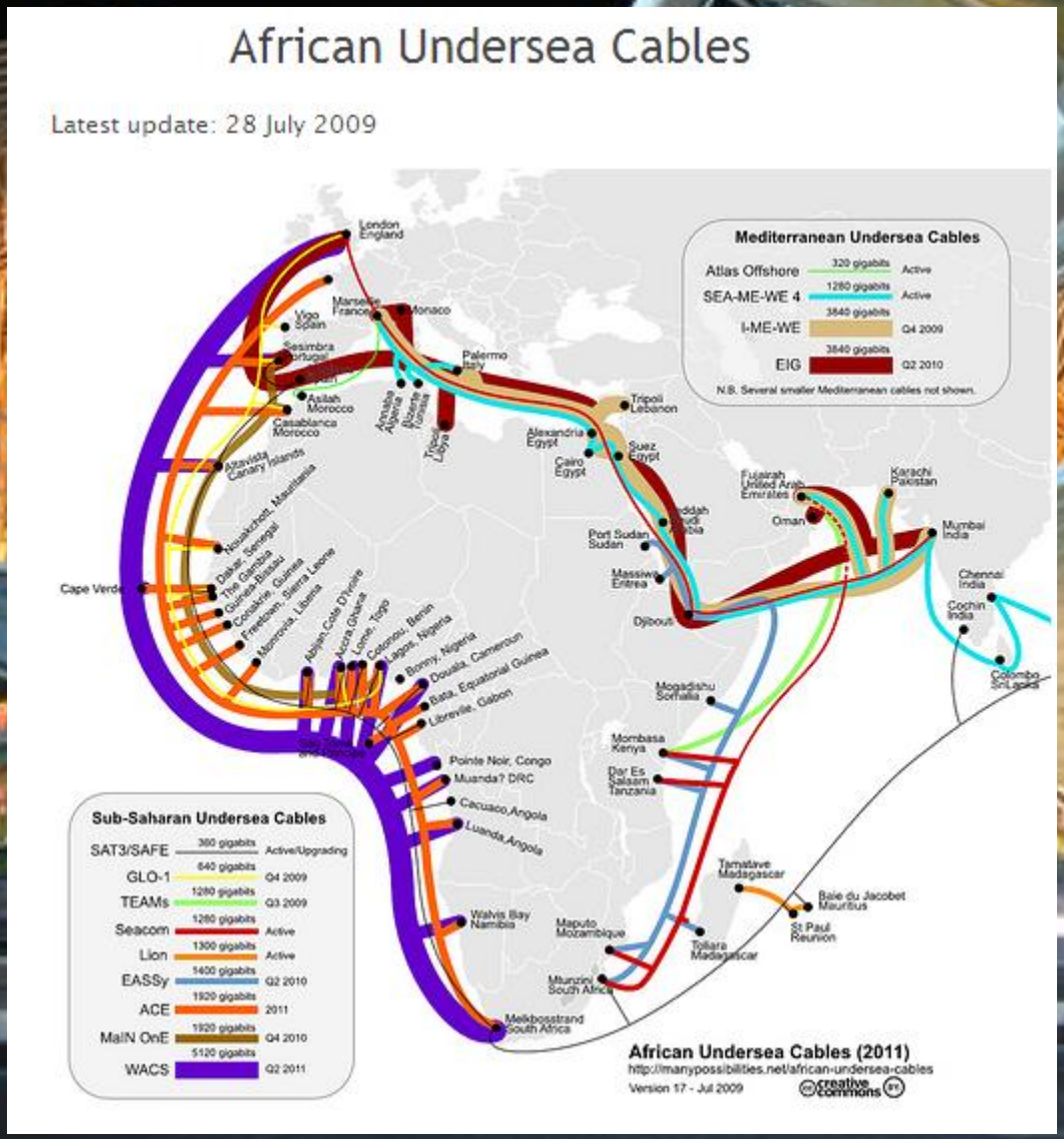
World Regions	Population (2009 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Penetration (% Population)	Users Growth 2000-2009	Users % of Table
Africa	997,269,930	4,514,400	64,153,900	6.4 %	1,321.1 %	3.9 %
Asia	3,822,428,903	114,304,000	700,863,930	18.3 %	513.2 %	42.1 %
Europe	803,490,338	105,096,093	402,380,474	50.1 %	282.9 %	24.2 %
Middle East	202,138,516	3,284,800	47,964,146	23.7 %	1,360.2 %	2.9 %
North America	340,831,819	108,096,800	251,735,500	73.9 %	132.9 %	15.1 %
Latin America/Caribbean	588,614,046	18,068,919	175,834,439	29.9 %	873.1 %	10.6 %
Oceania / Australia	34,853,867	7,620,480	20,838,019	59.8 %	173.4 %	1.3 %
WORLD TOTAL	6,789,627,419	360,985,492	1,663,770,408	24.5 %	360.9 %	100.0 %

NOTES: (1) Internet Usage and World Population Statistics are for June 30, 2009. (2) CLICK on each world region name for detailed regional usage information. (3) Demographic (Population) numbers are based on data from the US Census Bureau . (4) Internet usage information comes from data published by Nielsen Online, by the International Telecommunications Union, by GfK, local Regulators and other reliable sources. (5) For definitions, disclaimer, and navigation help, please refer to the Site Surfing Guide. (6) Information in this site may be cited, giving the due credit to www.internetworldstats.com.

Internet Users and Penetration (June 2009)



Internet in Africa



	Seacom	EASSy	TEAMs	WACS	MainOne	GLO1	ACE
Cost (millions of USD)	650	265	130	600	240	150	???
Length (km)	13,700	10,000	4,500	14,000	7,000	9,500	14,000
Capacity	1.28 Tb/s	1.4 Tb/s	120 Gb/s - 1.28 Tb/s	3.84 Tb/s	1.92 Tb/s	640 Gb/s?	1.92 Tb/s
Completion	July 2009	June 2010	Sept 2009	Q2 2011	Q4 2010	Nov 2009	2011

Quantifying the Internet

- Google indexed 26 Million pages in 1998 – today it indexes 1 Trillion pages
- There
- Amer
- Faceb

The Official Google Blog

Insights from Googlers into our products, technology, and the Google culture.

We knew the web was big...

7/25/2008 10:12:00 AM

We've known it for a long time: the web is big. The first Google index in 1998 already had 26 million pages, and by 2000 the Google index reached the one billion mark. Over the last eight years, we've seen a lot of big numbers about how much content is really out there. Recently, even our search engineers stopped in awe about just **how** big the web is these days -- when our systems that process links on the web to find new content hit a milestone: 1 trillion (as in 1,000,000,000,000) unique URLs on the web at once!

day and 53.8 tril

rches in Feb 200

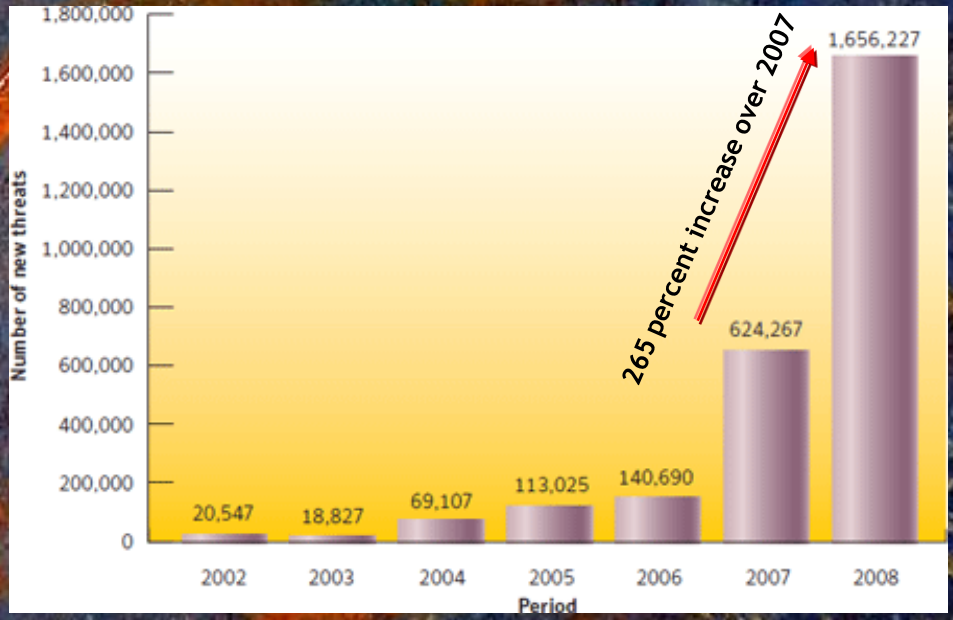
y 280 million

- Over 3 Billion pictures uploaded in Flickr
- Over 10 billion pictures uploaded on Facebook

Can we continue to trust the Internet?

- Cyber-threats, cyber-crime
- Complexity of critical Infrastructures
- Trust, accountability, transparency
- Identity, privacy and user empowerment
- Human values and acceptance

New malicious code signatures



350 Billion spam messages in 2008
94% of all e-mail
10 Million computers hijacked

Worms on Social Networks

- Kaspersky Lab revealsan increase in malicious programs, from 2.2 million in 2007 to 20 million in 2008.
- A new modification of Koobface was detected by the specialists at Kaspersky Lab on June 9 and became the 25 millionth malicious program added to the company's antivirus databases.
- The worm uses a simple propagation method: users of social-networking sites receive what appears to be a message from a friend containing a link to a video clip on an unknown site. When users attempt to play the video, they are prompted to update Flash Player. Instead of an update, however, a Koobface worm is installed that contains backdoor functionality allowing instructions from a remote management server to be run on the computer.

'Mafiaboy': Cloud Computing Will Cause Internet Security Meltdown

Notorious black-hat hacker warns that cloud-based computing will be "extremely dangerous," and explains how he got into hacking at age 15

juin 30, 2009 | 05:31 PM

By Kelly Jackson Higgins
DarkReading

Reformed black-hat hacker Michael Calce, better known as the 15-year-old "mafiaboy" who, in 2000, took down Websites CNN, Yahoo, E*Trade, Dell, Amazon, and eBay, says widespread adoption of cloud computing is going to make the Internet only more of a hacker haven.

"It will be the fall of the Internet as we know it," Calce said today during a Lumension Security-sponsored Webcast event. "You're basically putting everything in one little sandbox...it's going to be a lot more easy to access," he added, noting that cloud computing will be "extremely dangerous."

Cybercrime spreads on Facebook

Mon Jun 29, 2009 2:50pm EDT

By Jim Finkle - Analysis

BOSTON (Reuters) - Cybercrime is rapidly spreading on Facebook as fraudsters prey on users who think the world's top social networking site is a safe haven on the Internet.

Lisa Severens, a clinical trials manager from Worcester, Massachusetts, learned the hard way. A virus took control of her laptop and started sending pornographic photos to colleagues.

"I was mortified about having to deal with it at work," said Severens, whose employer had to replace her computer because the malicious software could not be removed.

Cybercrime, which costs U.S. companies and individuals billions of dollars a year, is spreading fast on Facebook because such scams target and exploit those naive to the dark side of social networking, security experts say.

While News Corp's MySpace was the most-popular hangout for cyber criminals two years ago, experts say hackers are now entrenched on Facebook, whose membership has soared from 120 million in December to more than 200 million today.

"Facebook is the social network du jour. Attackers go where the people go. Always," said Mary Landesman, a senior researcher at Web security company ScanSafe.

Scammers break into accounts posing as friends of users, sending spam that directs them to websites that steal personal information and spread viruses. Hackers tend to take control of infected PCs for identity theft, spamming and other mischief.

Hacker conference announces internet security flaw

Josh Smith

Aug 3rd 2009 at 10:00AM

Filed under: Technology

Just when you thought it was safe to go online, the hackers at Def Con announced a new security flaw regarding the way websites prove their validity.

Currently, websites that deal with personal information make use of SSL technology to maintain a secure connection. You may be more familiar with SSL security by the little padlock icon that shows up in most browsers or the "s" that follows "HTTP" in a web address. Generally these indicators mean that anything you transmitted to the website was secure, but these newly found flaws allow for someone to tap the connection.

Basically this flaw lets a hacker trick your web browser into not looking further at a web address that has a special character in it, letting unscrupulous individuals pose as a legitimate site. From there they can collect personal information and even install software on your computer.

U.S. Government's Cyberdefense System Doesn't Work

Wednesday, July 08, 2009
THE WALL STREET JOURNAL.

The flagship system designed to protect the U.S. government's computer networks from cyberspies is being stymied by technical limitations and privacy concerns, according to current and former national-security officials.

The latest complete version of the system, known as Einstein, won't be fully installed for 18 months, according to current and former officials, seven years after it was first rolled out.

This system doesn't protect networks from attack. It only raises the alarm after one has happened.

A more capable version has sparked privacy alarms, which could delay its rollout. Since the National Security Agency acknowledged eavesdropping on phone and Internet traffic without warrants in 2005, security programs have been dogged by privacy concerns.

In the case of Einstein, AT&T Corp., which would test the system, has sought written approval from the Justice Department before it would agree to participate, people familiar with the matter say.

An AT&T spokesman declined to comment.

The total cost of the system, designed to protect all nonmilitary government computers, is classified, but officials familiar with the program said the price tag was expected to exceed $2 billion.

• Click here to read the rest of this story in the Wall Street Journal.

Government Recruits Geeks to Blunt Cybersecurity Threats

The U.S. Cyber Challenge aims to identify 10,000 patriotic geeks and make them experts

By Joshua Kucera
Posted August 6, 2009

The potential threats against the United States from malicious foreign hackers are as poorly understood as they are scary. China's military has trained more than 60,000 "information troops," and its official doctrine calls for pre-emptive strikes on networks of nations it sees as a threat. Russian hackers—probably with Kremlin support—have attacked Internet sites in pro-Western Estonia and Georgia. And a mysterious "worm," Conficker, infects an estimated 5 million computers around the world. Authorities don't know who controls it; cyberintelligence expert Jeffrey Carr calls it "the equivalent of a nuclear bomb" that could shut down the entire Internet.

It's the kind of shadowy, nonstate threat that the U.S. defense and intelligence bureaucracies are traditionally ill equipped to fight, but a new initiative announced last week aims to try. A consortium of government agencies and private organizations has set up a series of competitions, called the U.S. Cyber Challenge, to identify up to 10,000 patriotic geeks and then nurture them to become "top guns," as the Cyber Challenge organizers call them, at the Pentagon, the National Security Agency, and elsewhere.

The Department of Defense trains only about 80 cybersecurity experts a year, far fewer than what are most likely needed. "People in the Pentagon know that the guy who looks good in a flight suit and can do 100 push-ups isn't necessarily the guy who will be the world's best hacker," says Noah Shachtman, editor of *Wired* magazine's Danger Room blog, who has briefed Pentagon officials on cyberwarfare. "So they know they have to reach out beyond traditional military recruiting models to find the top people. They're not sure exactly how to do it, though, and this is one attempt."

August 29, 2009 - 8:25 A.M.

Obama's 'emergency' powers over Internet: Cybersecurity Bill S. 773

1 comment

TAGS: Barack Obama, cybersecurity, Obama, S. 773, White House

IT TOPICS: Careers, Cybercrime & Hacking, Government & Regulation, Internet, Security

It's proposed that the White House should have emergency powers to control the Internet. A bill would give Barack Obama 'cybersecurity' authority to disconnect users and professionally certify IT people. In *IT Blogwatch*, bloggers get *really* spun up about it.

Digg

submit

By Richi Jennings. August 29, 2009.

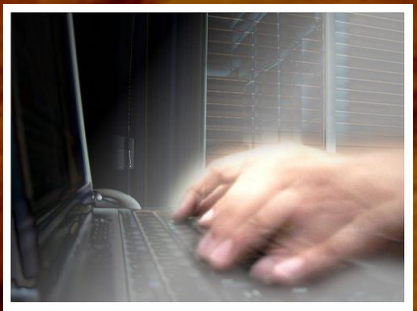
Your humble blogwatcher has selected these bloggy morsels for your enjoyment. Not to mention *boycotting Scotland*...

Declan McCullagh takes liberties:

> Internet companies and civil liberties groups were alarmed this spring when a U.S. Senate bill proposed handing the White House the power to disconnect private-sector computers from the Internet. They're not much happier about a revised version. ... CBSNews.com has obtained a copy.
> ...
> The new version allows the president to "declare a cybersecurity emergency" relating to "non-governmental" computer networks and do what's necessary to respond to the threat. Other sections of the proposal include a federal certification program for "cybersecurity professionals," and a requirement that certain computer systems and networks in the private sector be managed by people who have been awarded that license.

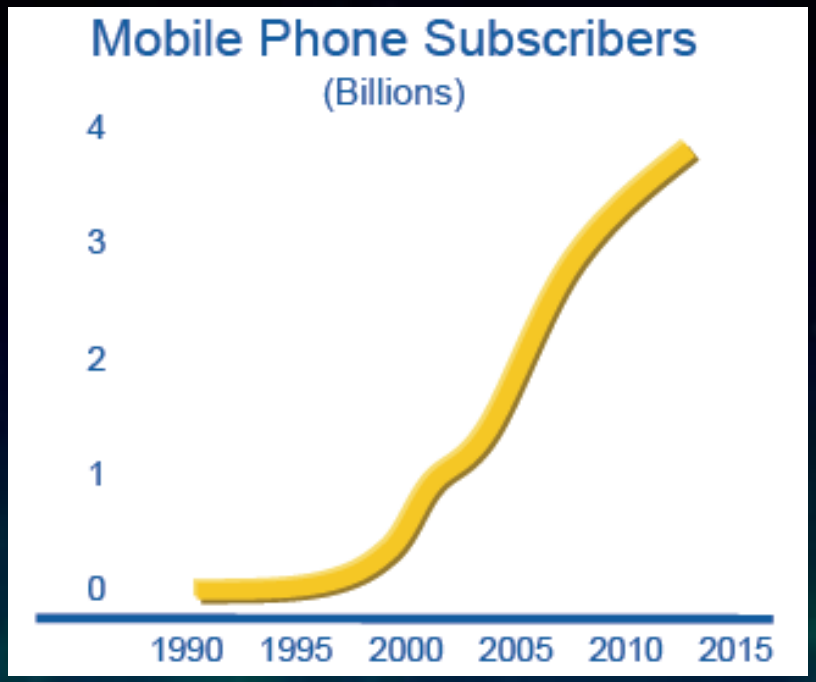
The Hadopi story

- Bill will allow for the punishment of ISP account holders for copyright infringing
- However an IP address does not necessarily identify an individual,
- In many instances it doesn't even identify a computer but merely a gateway to a sub network, behind which could be any number of individuals not linked in any way to a bill payer.
- The Hadopi Router, locates Wi-Fi networks in the neighbourhood, and cracks all their passwords. Once the keys are found, a virtual access point is created – i.e an Internet connection without the account holder's knowledge



http://www.routeurhadopi.fr/

The Internet is going wireless



Power-limitation of handheld - computation will move to the cloud

Need to back up and refresh our lost data - data will move to the cloud

Search and Find

- Real Time
- Event driven

(Relationships among objects and attributes)

- Twitter of Things
- Search Market dominance

How can a network (or device) anticipate my search?

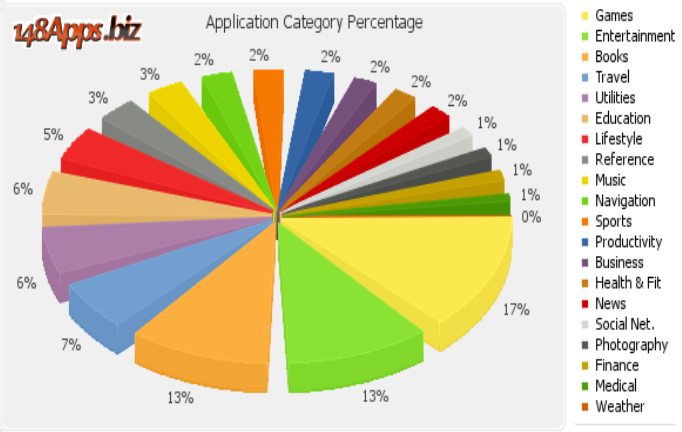
"Network push" => human-centered "demand pull"

Speed and the dynamics of change are unprecedented

iPhone generated 33 percent of smartphone traffic worldwide and 50 percent in the US.

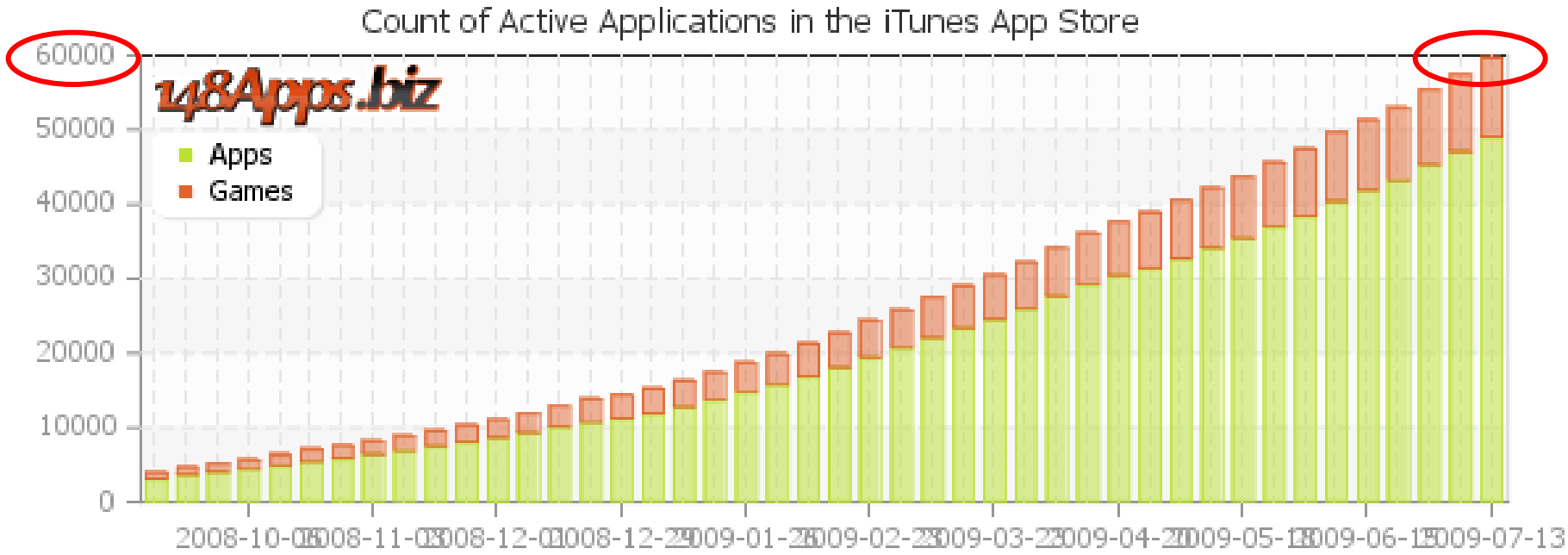
Applications market goes Mobile

Count By Price - Active Apps				
App Price	**# Apps**	**# Games**	**Total**	**% of Total**
Free	12,798	3,539	16,337	(23.06%)
0.99	26,218	5,897	32,115	(45.33%)
1.99	6,528	1,688	8,216	(11.60%)
Total # apps:	**58,265**	**12,579**	**70,844**	**(100.00%)**
Total cost to buy all apps:	**$159,623.33**	**$17,556.60**	**$177,179.93**	
Average App Price	**$2.74**	**$1.40**	**$2.50**	

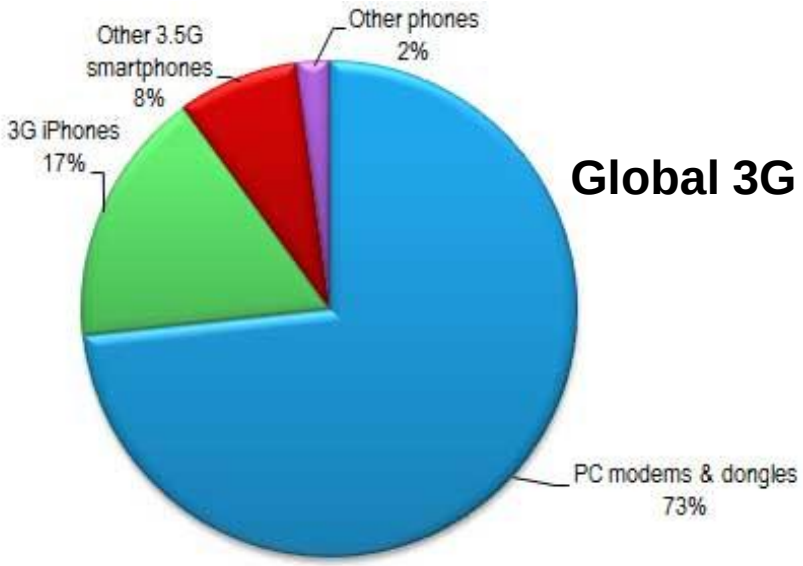


1.5 Billion iPhone Apps Downloaded
Estimated value $2.5Billion

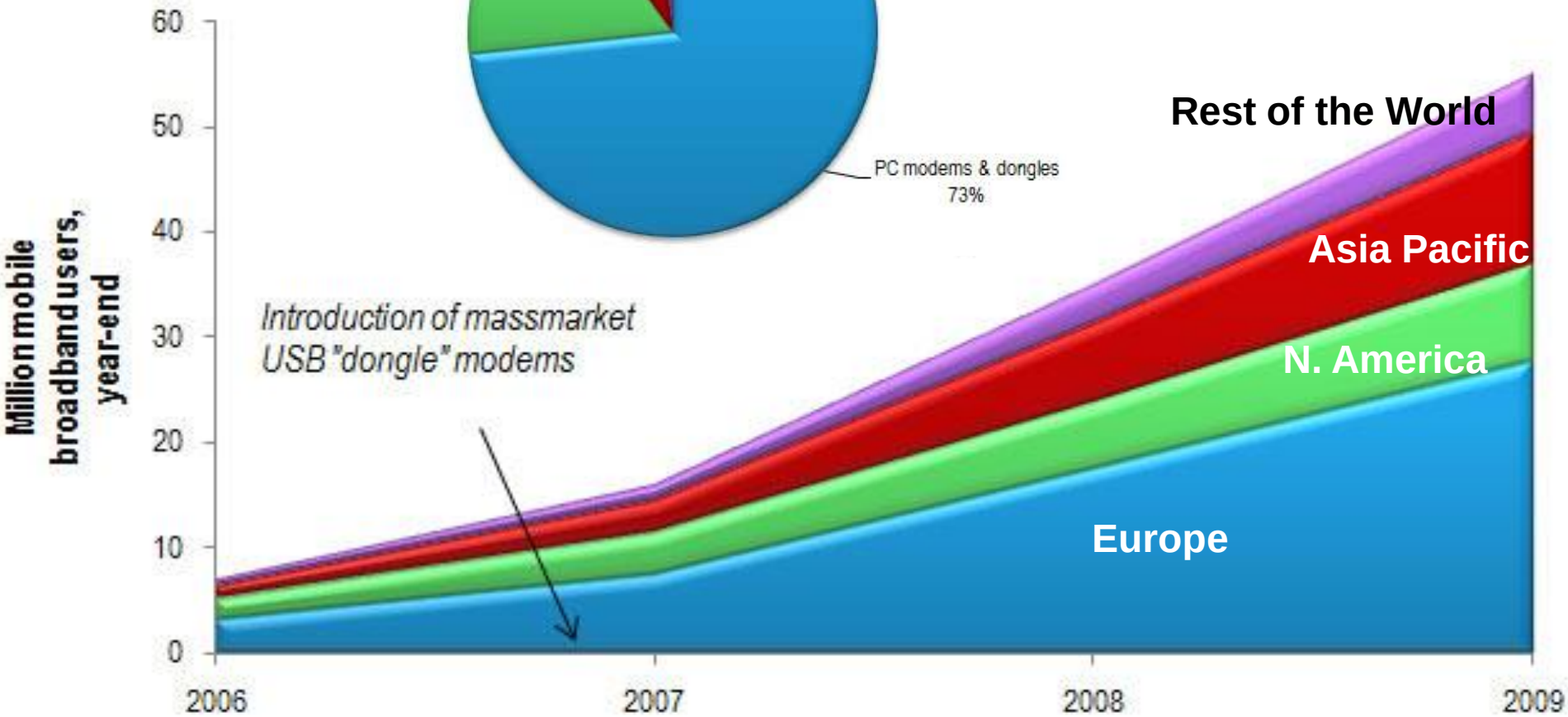
Page last updated: 2009-08-27 02:55:15 -0700 PDT



Global mobile broadband



Global 3G data traffic by device type

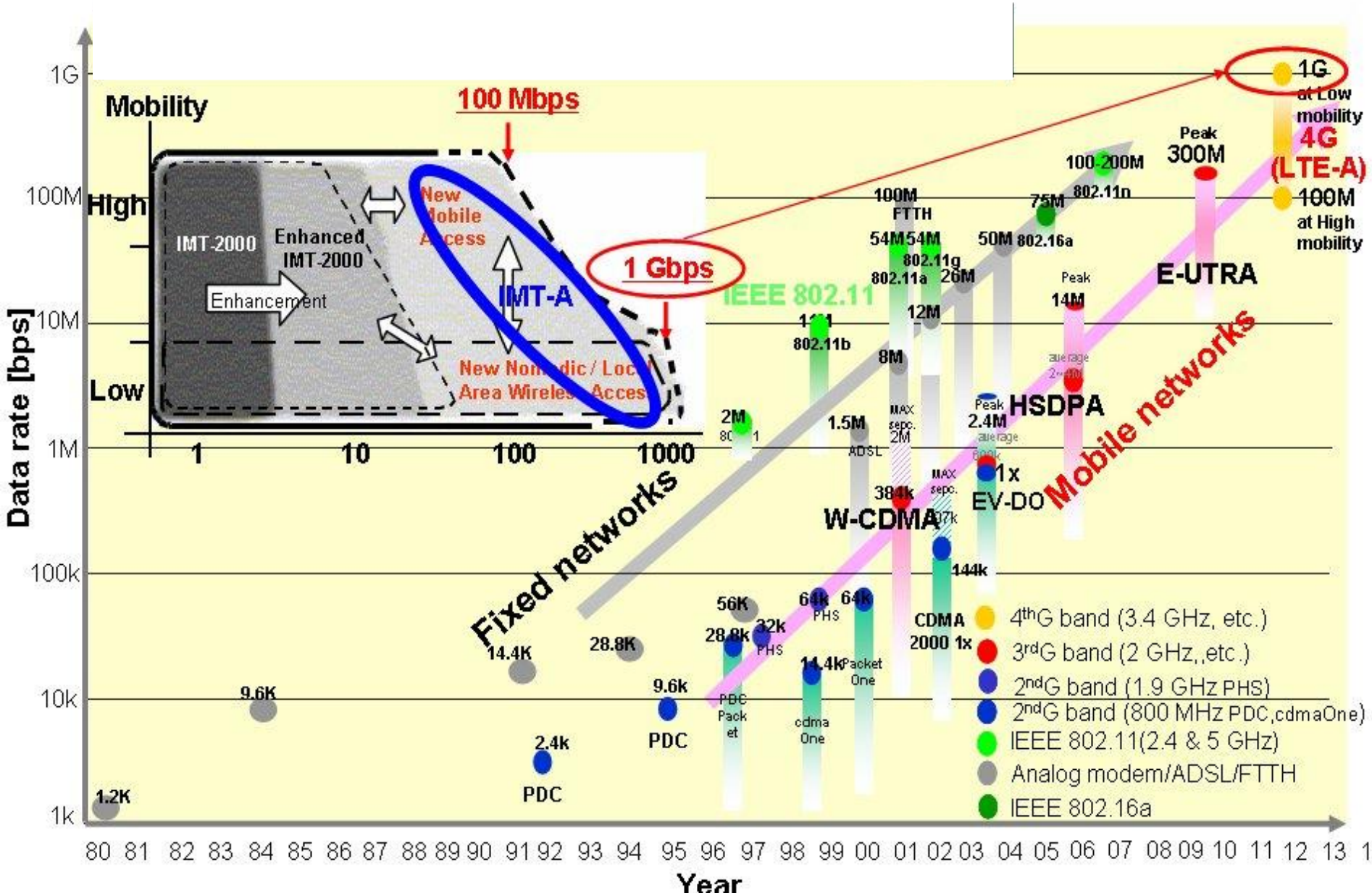


Arrival of the broadband mobile Internet

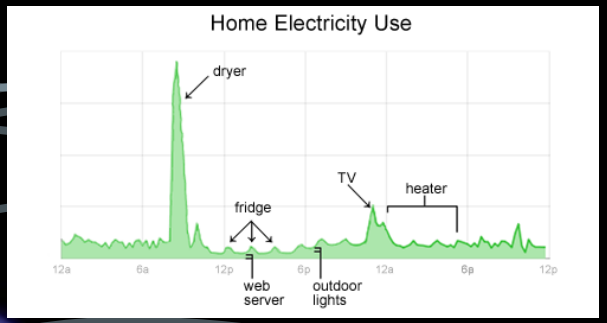
The arrival of very high speed and all-IP mobile networks is imminent. So-called 4G will transform markets and the mobile services paradigm worldwide.

- **The Promised Land is at hand**
  - **LTE field tests achieving "ultrabroadband" speeds of 160-250MB/s down, 50 MB/s up**
  - **Commercial shipments have begun**
- **How will a "mobile broadband Internet" be different?**
  - **For the consumer experience?**
  - **For service definition?**
  - **For the competitive landscape?**

Coming-up “LTE advanced”



The Internet of Things



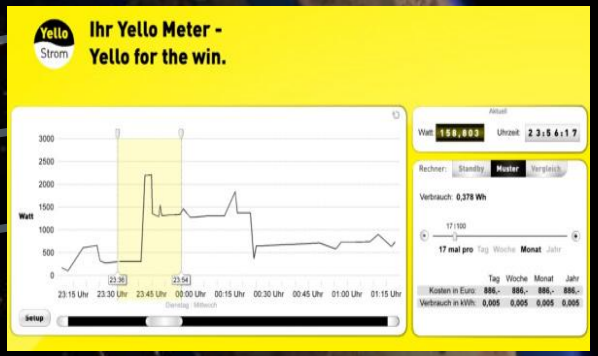
Anytime

Anywhere

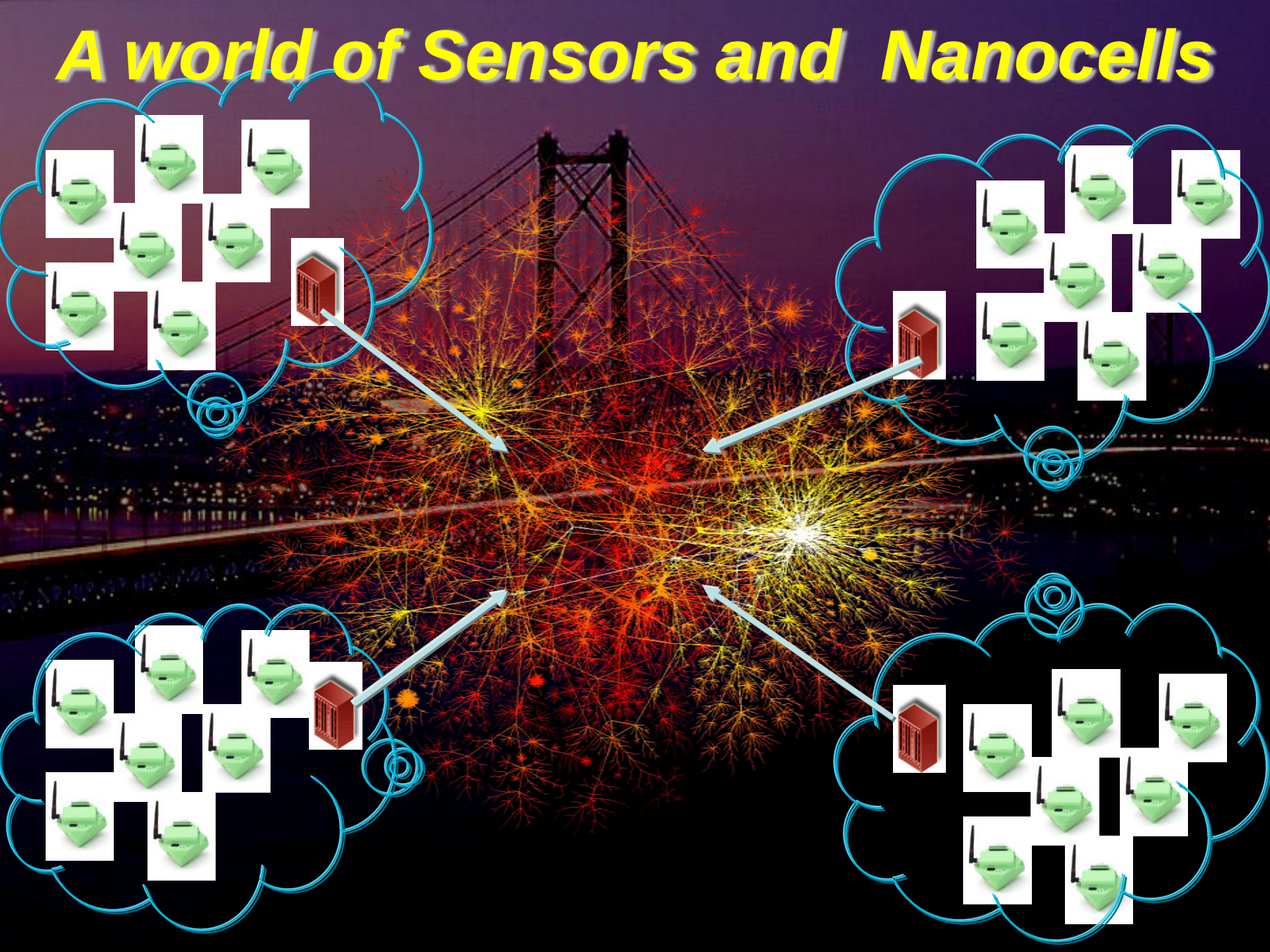
Anyway

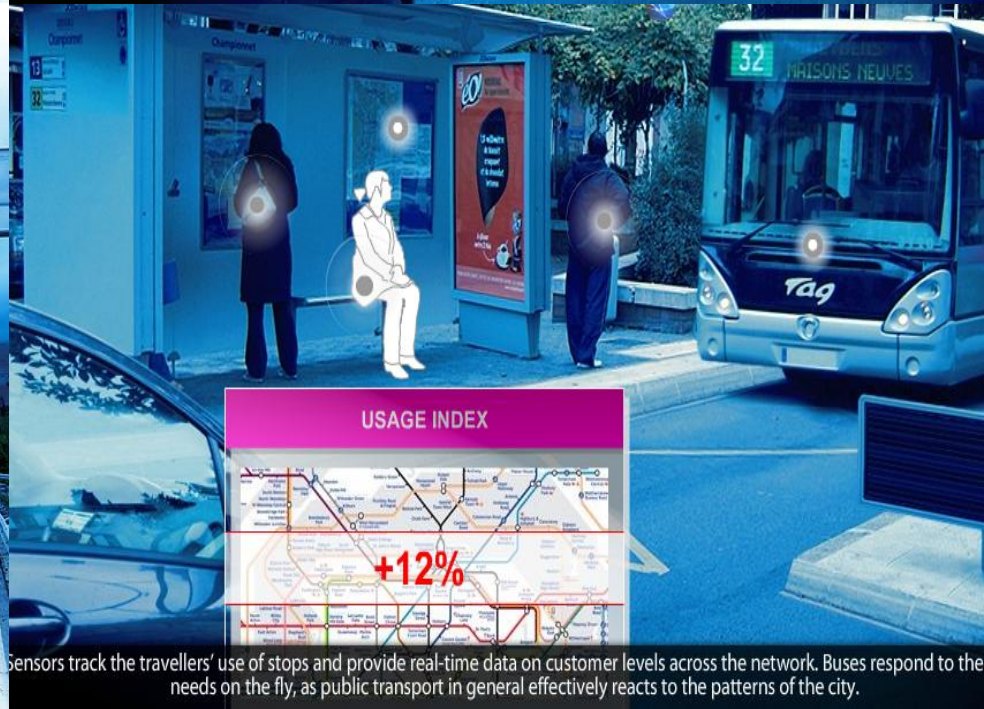
AnyThing

- Use sensors to create events.
- Infrastructure to create and link all such events.
  - Index
  - Search
  - Present
- Capture events and put them on the Web.



A world of Sensors and Nanocells





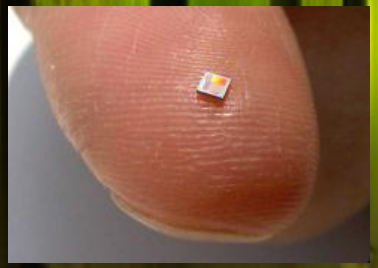
Sensors track the travellers' use of stops and provide real-time data on customer levels across the network. Buses respond to the needs on the fly, as public transport in general effectively reacts to the patterns of the city.

While she was in the bus Alice received a message inviting her to switch to a bike at next station to shorten the travel. She has a permanent monitoring of the saved time depending on which of the travel mode switches she has selected.

Ticket prices are recalculated continuously depending on multiple factors. People gain 'carbon credits' by using public transport regularly and the credit is carried over into their overall 'sustainability index'.

Internet of Things, Issues to resolve

- Architecture (servers, discovery services etc)
- Governance, naming, identity, interfaces
- Service openness, interoperability
- Spectrum
- Standards



The "Information Shadow" and the Internet of Things

- Emails, instant messages, phone calls, tweets, blog postings, photographs, videos, all leave traces.
- A product on the supermarket shelf or a car on a dealer's lot, all have information shadows now.
- In many cases, these information shadows are linked with their real world analogues by unique identifiers e.g. RFID and IP addresses).
- There is however no need for unique identifiers to be assigned.
- A picture of its label taken by your mobile phone, coupled with image recognition, search, and the web will do the rest.

Disappearing in the digital age

http://www.wired.com/vanish/

- ***"where once you could move a few states over, adopt a new name and live on with minimal risk, today your trail is littered with digital breadcrumbs dropped by GPS-enabled cell phones, electronic bank transactions, IP addresses, airline ID checks, and, increasingly, the clues you voluntarily leave behind on social networking sites*.**

- **Wired is organizing a hunt for missing writer Evan Ratliff with a $5000 reward. He wrote a piece about disappearing I the digital age and is trying to stay hidden until September 15.**

Vanished and Captured: Recapping the Hunt for Evan Ratliff

By Nicholas Thompson ✉ September 10, 2009 | 6:49 pm | Categories: Wired Issue 17.09

How hard is it to shed one's skin in the age of Facebook and Twitter, and how do investigators track down the thousands of people who do this each year? In the September issue of *Wired* magazine, contributing editor Evan Ratliff wrote a story about disappearing in the digital age.

When the magazine hit newsstands on August 15, Evan took off, too. *Wired* offered $5,000 to anyone who could find him, with $3,000 going to Evan if he made it a month undiscovered. To make the hunt fair, I had access to all of Evan's credit-card, bank and personal accounts, and I posted his transactions and e-mails online. Meanwhile, Evan was required to act like a person who really wanted to start his life over again: He had to create false accounts online, stay in cities and live in a way he would if truly starting life anew.

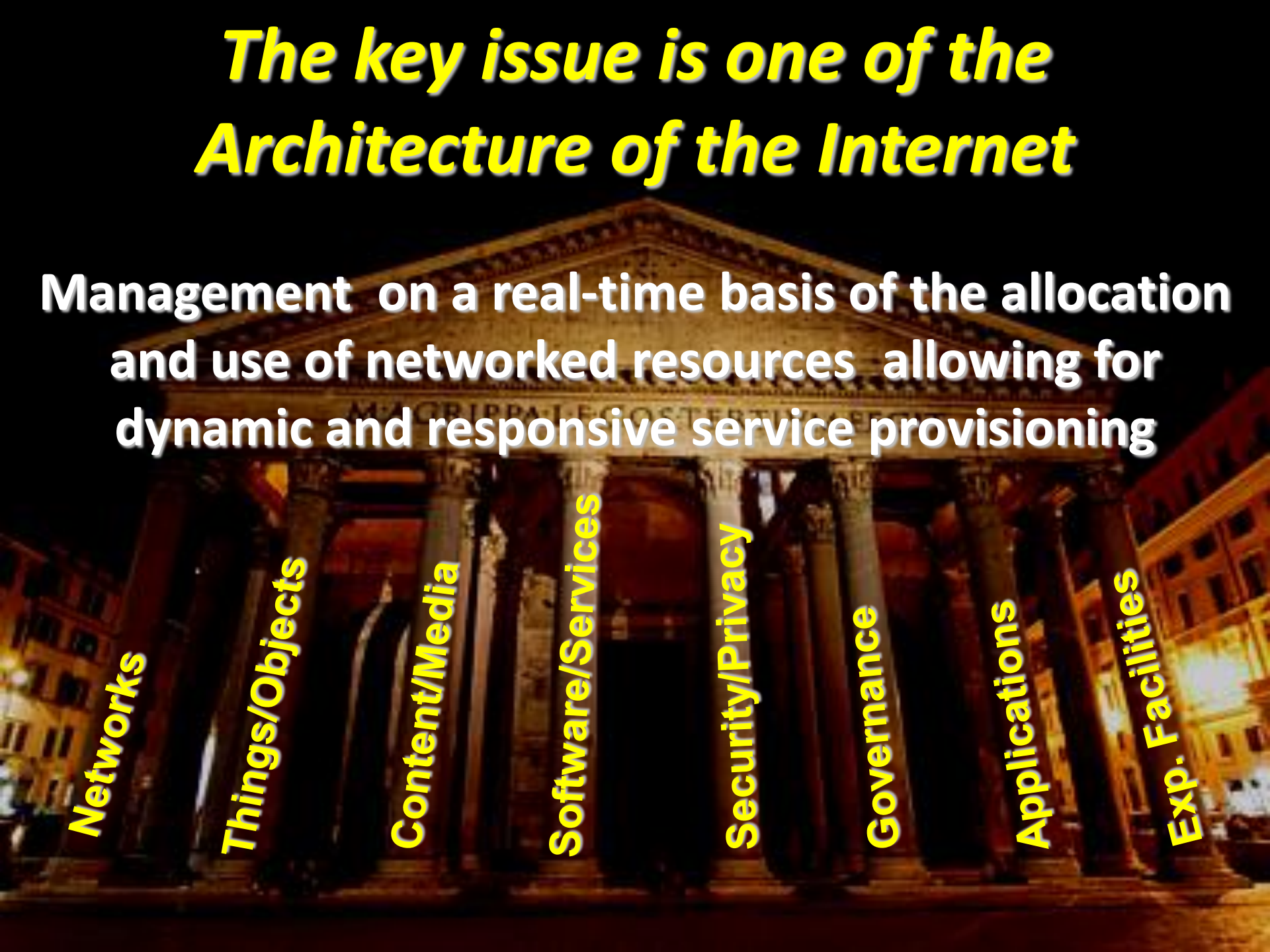
Summing up the hunt

What followed Evan's disappearance was the most fun journalistic experience I've ever participated in. Evan began by leaving a few clues about his location: He sold his car in Las Vegas, pulled money out of an ATM in Santa Monica and even snuck into an interview on Venice Beach with Sometimes Daily.

Meanwhile, the hunt grew. The Facebook group devoted to finding Evan expanded to about 1,000 members and a

The key issue is one of the Architecture of the Internet

Management on a real-time basis of the allocation and use of networked resources allowing for dynamic and responsive service provisioning

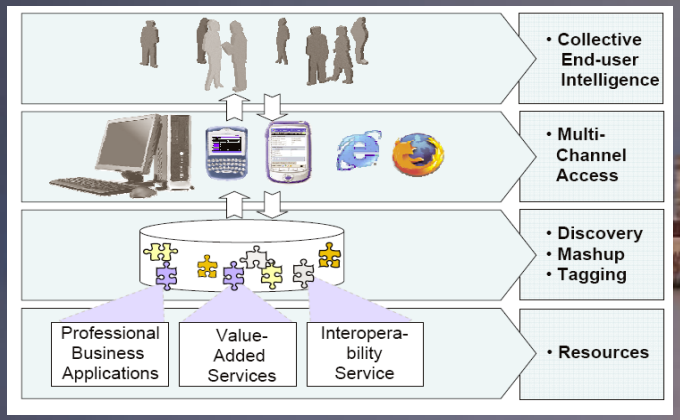


The Internet is under Multiple Threats

- Current architectures give rise to increasing opportunities for “Lock-ins” e.g., device, operator lock-in, frequency lock-in, network lock-in, identity lock-in
- Innovative business models may be stifled
- Current architectures are massively open to security breaches, privacy invasion and identity theft
- Emergence of parallel, heterogeneous architectures whose interoperability is difficult if not impossible to ensure, operate or maintain
- Current infrastructures will not be able to handle, scalability and bandwidth demands

Future Internet requires a systems perspective

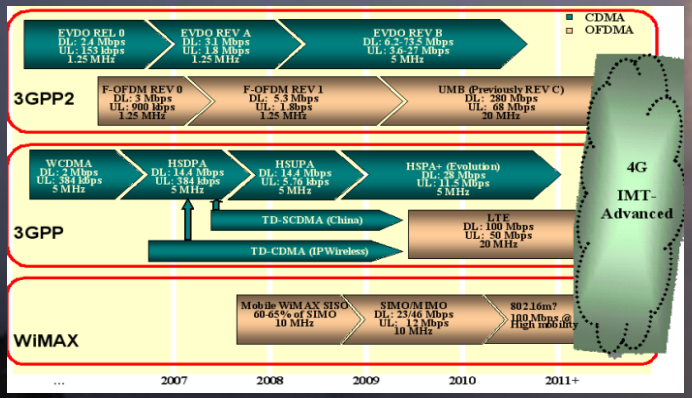
Internet of Services, Service Web



3D Internet

Trust

Security



Networks of the Future

Internet of Things

Internet is needed to make the World Smarter

Smarter Transportation

Smarter Education

Smarter Food Systems

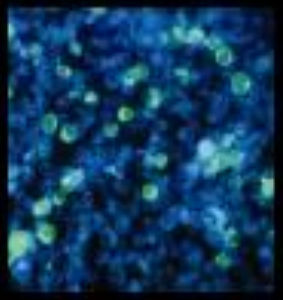
Smarter Healthcare

Smarter Energy

Smarter Retail

Smarter Countries

Smarter Government Services



Smarter Water

Smarter Public Safety

Smarter Regions

Smarter Cities

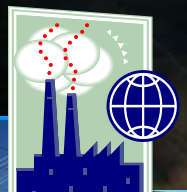
FI represents an opportunity for Europe

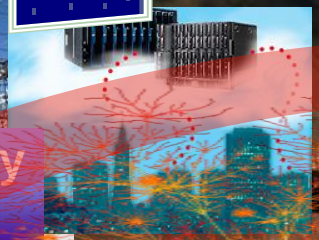
- **Key technological drivers are EU domains of excellence**
  - mobility, security, broadband, sensors.
- **Prospects for regaining ground in Internet related fields**
- **Clear multiplier prospects:**
  - downwards, towards the components and subsystems
  - upwards, towards innovative service industry
- **However a clear European strategy is needed**
  - to pool resources across Europe
  - to respond to the multiple new requirements coming from the variety of sectors involved
  - to create the right economic opportunities in Europe

So what is the EC doing?

- **Investing on R&D**
  - Over 100 on-going projects
  - In excess of 500 Million Euros already committed
  - Currently some 30 new projects are under negotiation
  - Additional 200 Million Euros to be committed before year end
  - Call 5 closing 26 October will add some 70 new projects worth over 300 Million Euros
- **Setting the right regulatory conditions**
  - New regulatory framework proposed
  - Recommendation on RFID
  - Communication on IoT
  - Communication on Future Internet and PPP (~~22 September 2009)
- **Launching a Public Private Partnership with 300 Million Euros for the next 3 years to look into the applications space that can be enabled by the Internet**

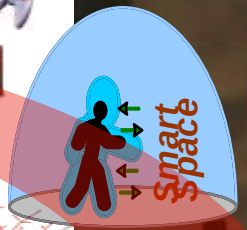
Which Applications?





Smart Energy Networks

Smart Living



Smart Transport Networks

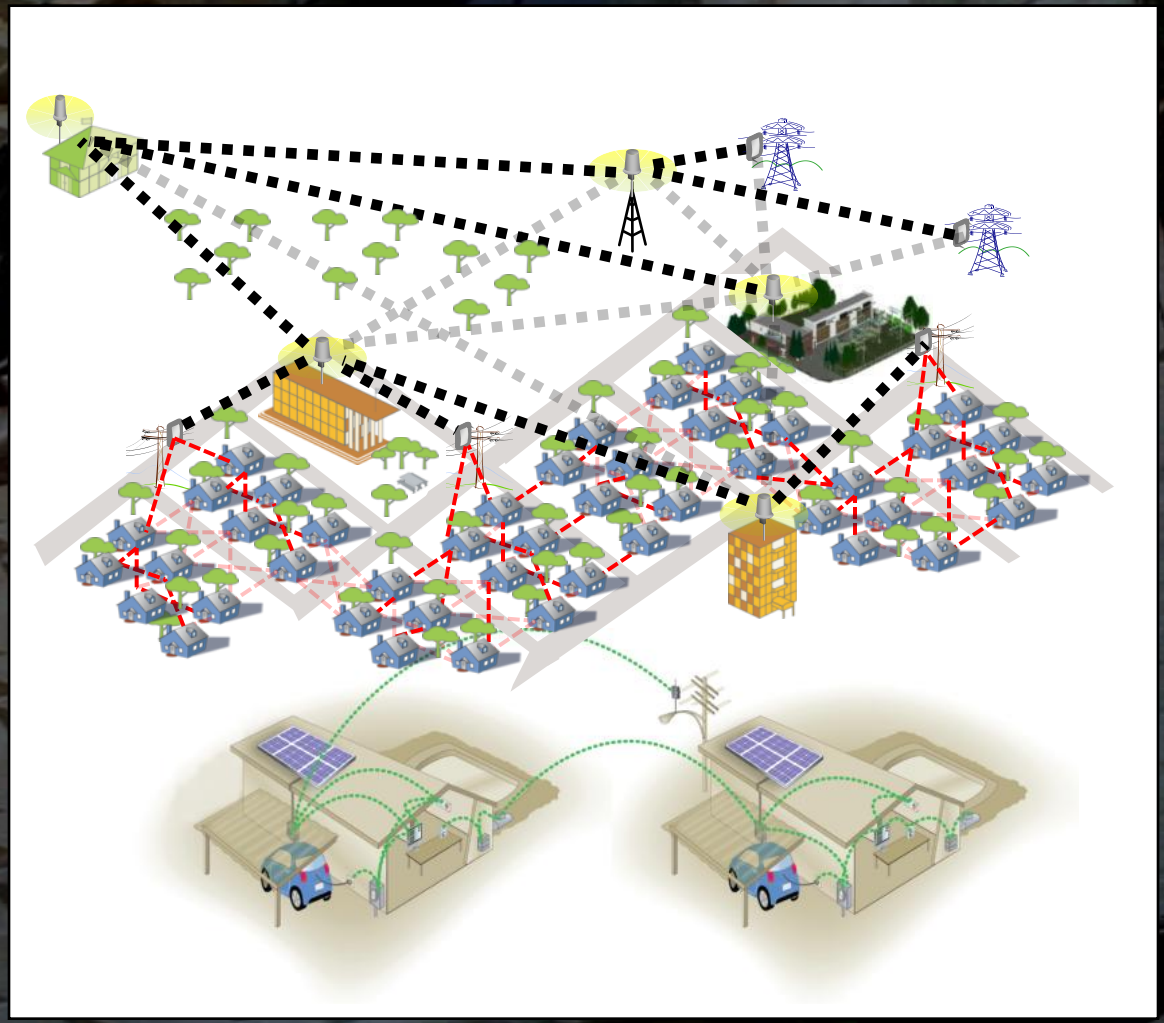
eHealth & Smart Health networks

E.G. Smart Grid

Broadband Network Tier (WAN)

Neighborhood-Area Network (NAN)

Home-Area Network (HAN)



E.G. Real Time Traffic Monitoring

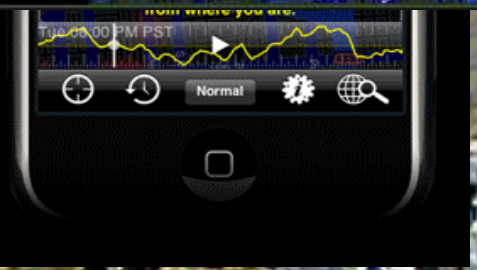
- Real-time traffic monitoring systems like reduce wasted time and energy commuting.
- Web services reporting progress of buses and trains against their scheduled times make public transit more effective.
- Instrumenting the world brings clear consumer benefits from. Sensor-driven congestion pricing schemes like the one in use in Stockholm create economic incentives to reduce traffic at peak times.

E.G. Sensing the City

Where is everybody?

- How busy is the city? Know when to go out
- See the top nightlife hotspots in real-time
- Find out what's there in one click
- Find out where everyone's going next

>> More info



http://www.citysense.com/home.php

As a final observation

- Internet disruptions will be plenty
- We have a unique opportunity to put Europe ahead of the game
- Structural changes and an open innovation attitude are needed
- Ambition and commitment to act are an imperative

Further Information

http://ec.europa.eu/information_society/activities/foi/index_en.htm

http://www.future-internet.eu/home.html

Further Documentation

- **COMMISSION RECOMMENDATION of 12.5.2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification**
- **COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS of 18.6.2009 on Internet of Things — An action plan for Europe**
- **PUBLIC CONSULTATION "Transforming the digital dividend opportunity into social benefits and economic growth in Europe" from 10.07.2009 to 04.09.2009**
- **COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS** "A public-private partnership on the Future Internet"