FUTURETEXT

Mobile Web 2.0 workshop

Ajit Jaokar - many hats

FUTURETEXT

Ajit Jaokar

UK based - Hands on Publisher (futuretext) - Author (Mobile Web 2.0) - Chair: Oxford University's Next Gen Mobile Applications panel - PhD student UCL/UK

Recent and forthcoming talks include
Mobile world congress, Stanford University - MIT

Sloan - Web 2.0 expo - Ajaxworld

Supernova - CNN money - BBC - Oxford University European parliament

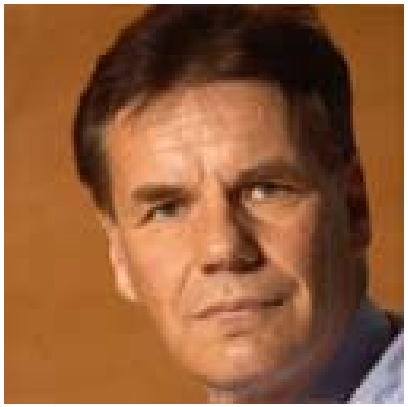
web2.0 workgroup

University of Oxford Continuing Education
Delivering learning online

Global top 20 wireless blogger
According to fierce wireless
www.opengardensblog.futuretext.com

Mobile Mobile Mobile ..

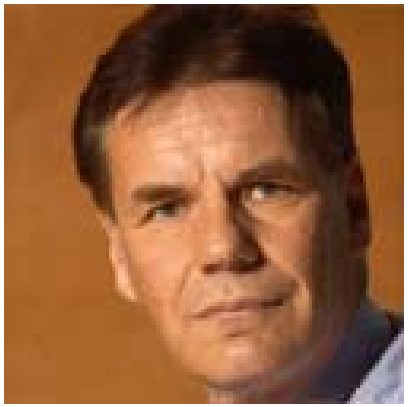
FUTURETEXT



Mobile Mobile Mobile .. Eric Schmidt - Google

Nokia is going to be an Internet company - Nokia chairman Olli-Pekka Kallasvuo

How can big and small developers get their apps on the iPhone - Steve Jobs - Apple



Why is Mobile Web 2.0 important?

iPhone, Android, Nokia are looking at the Web and the Mobile Web together ..

FUTURETEXT

Introductions: Name, Designation, Company, what you hope to gain, what you hope to contribute

Social networking – the Basics
Principles of Web 2.0
Mobile Web 2.0
The unique elements of Mobile Web 2.0
Mobile Web 2.0 and IMS (Telecoms operator viewpoint)
Mobile Web 2.0 and the Enterprise
Mobile Web 2.0 and browser extensions (DOM extensions)
Mobile Web 2.0 and device APIs
Other implementations of Mobile Web 2.0(smart card web server, devices etc)

Mobile Web 2.0 and Open social networks
Mobile Web 2.0 and Android
Mobile Web 2.0 and the iPhone

A lot of ground to cover ..

Emphasis, Learning and enjoying!

Participation – Three books ☺

Staying later on first day

Web 2.0 – the machine is Us/ing us

http://www.youtube.com/watch?v=6gmP4nk0EOE

Web 2.0 – Tim O Reilly

http://www.youtube.com/watch?v=CQibri7gpLM&feature=related

When Basecamp asked 1000 of their customers what Web 2.0 meant to them:

- **13% answered that they didn‘t know what it was**
- **87% who answered yes on the question, nearly everybody came up with a different description**

Many technologists don't get Web 2.0(Web 2.0 = Ajax?)

Tim Berners Lee: *nobody even knows what it means*

FUTURETEXT

- **Power is moving away from the old elite (Rupert Murdoch, CEO NewsCorp.)**

- **Our industry is facing a profound challenge from home-made content (Tom Glocer, CEO Reuters)**

But some people definitely do!

The formal definition : O'Reilly Definition

FUTURETEXT

"Web 2.0 is the network as platform, spanning all connected devices; Web 2.0 applications are those that make the most of the intrinsic advantages of that platform: delivering software as a continually-updated service that gets better the more people use it, consuming and remixing data from multiple sources, including individual users, while providing their own data and services in a form that allows remixing by others, creating network effects through an "architecture of participation," and going beyond the page metaphor of Web 1.0 to deliver rich user experiences."

- Strong User generated component
- Strong 'social' use of the web
- Element of 'Sharing'/'Free'
- Yet, useful applications (Flickr v.s. petfood.com)
- Services predominantly free but ad funded
- Coined by Tim O Reilly at a conference in 2004
- Official definition of Web 2.0 as above (although there are many other definitions)
- Even if you think it is hype (which I do not think so), it is a very good lexicon

At a minimum, Web 2.0 can be characterised by three properties

a) The use of the Web as a backbone
b) Harnessing collective intelligence and
c) Creating a database/body of data that becomes richer as more users contribute to the system .

What is Web 2.0

a) Web as a platform:

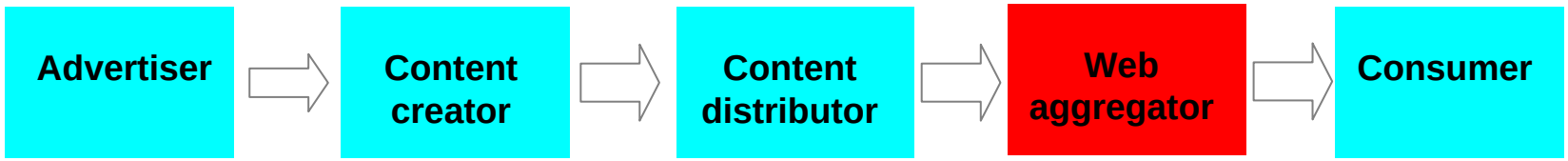
b) Harnessing collective intelligence : Google page rank

The platform is the Internet,
On the Internet, the rules are different.
Information sharing is actually better than information hoarding.

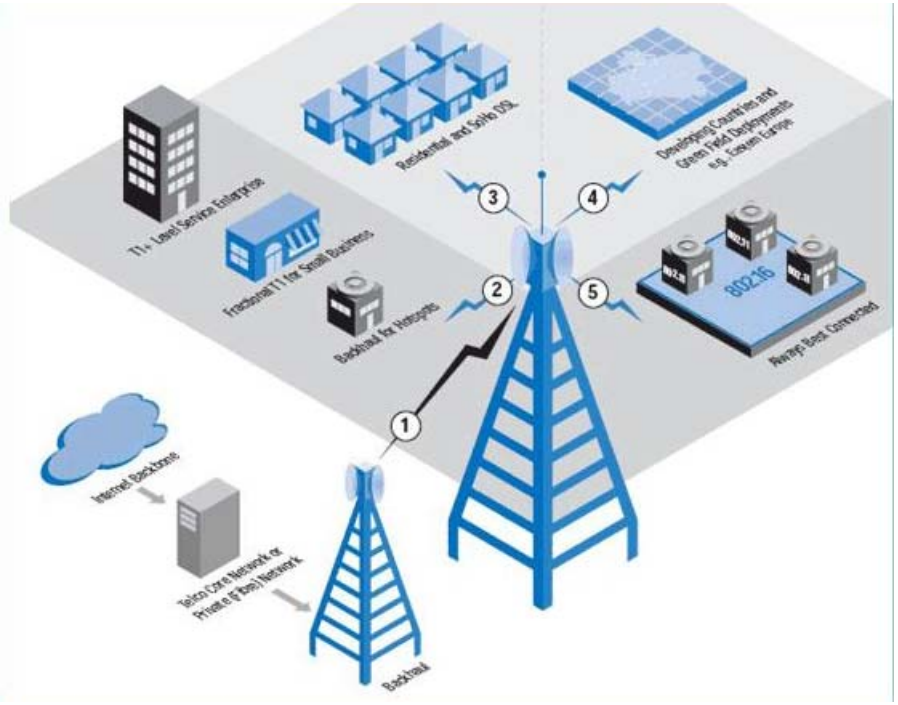
With enough people sharing information – you build a database and the database becomes bigger and better with incremental users

Value chain ..

FUTURETEXT



Web aggregators is a different type of distributor. Everyone is trying to bypass the traditional distributors. Distributors are having to evolve. Dis-intermediate …



Advertiser ⇨ **Content creator** ⇨ **OPERATOR** ⇨ **Web aggregator** ⇨ **Consumer**

The Operator is a type of distributor and is facing the same problem which other distributors are facing

A fork in the road for former partners?

FUTURETEXT

DIS-tributor v.s. Dis-Intermediate

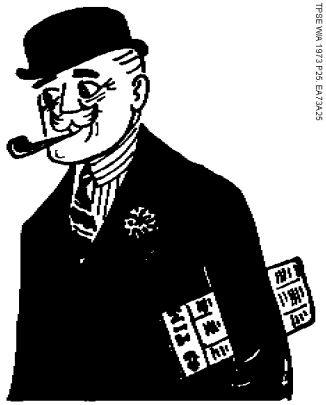
Content creator

Customer

Content distributor

OPERATOR

Where is the growth going to come from in our industry?



Web growth is proven.
Mobile Web growth is not.
Can Mobile Web 2.0 help?

http://www.pipes.org/Ephemeris/ea73/ea73a25.gif

http://www.finfacts.com/irelandbusinessnews/uploads/googmsftnov212006.jpg

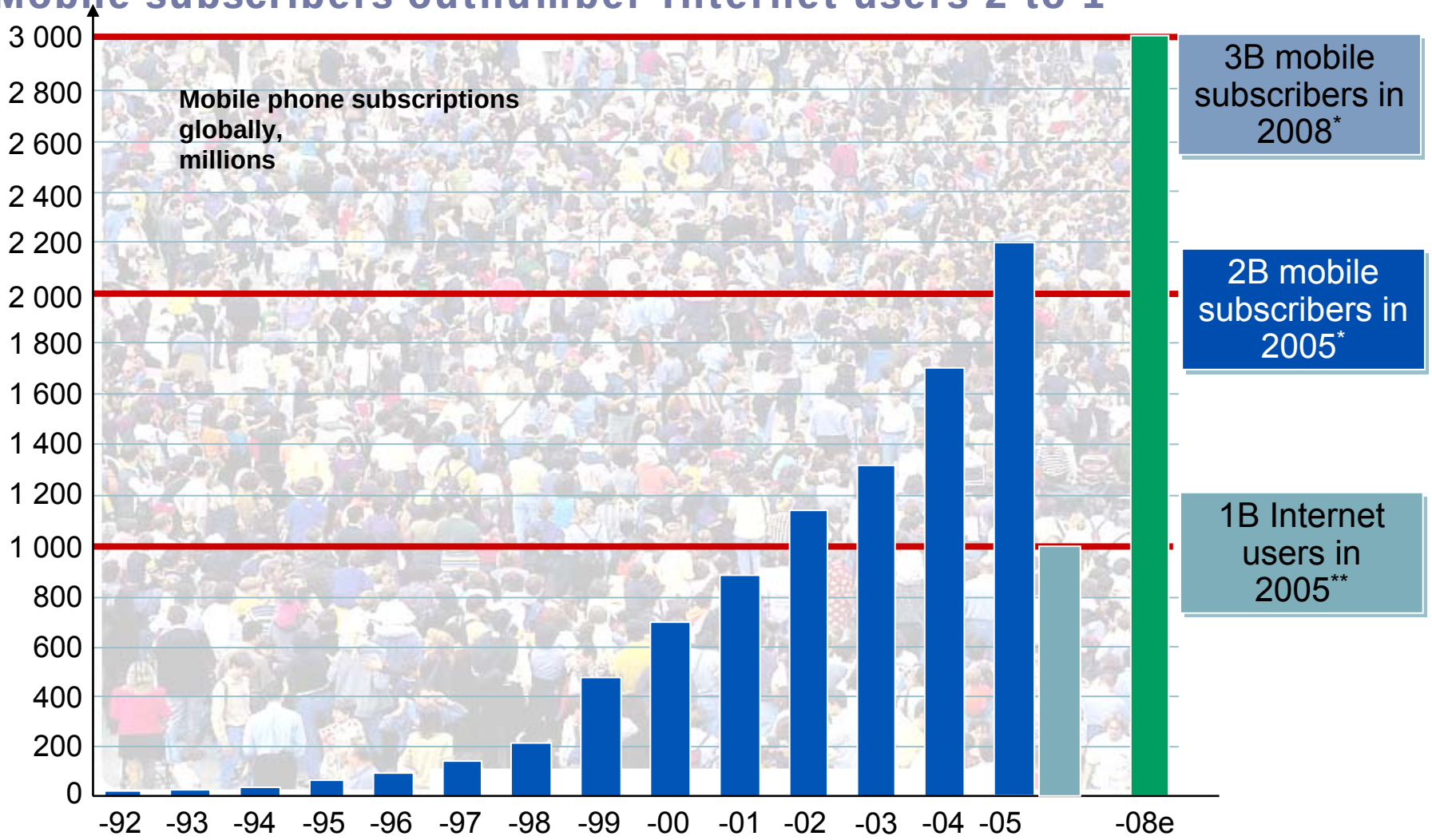
Changing worlds ..

FUTURETEXT

- 99% reliability
- 18 months lead time
- Silo mentality
- Interoperability – not a priority
- Data apps: low priority

- No unpipe
- Social networks, Connecting people vs. the media industry
- Iterative development, Converged development
- Network itself is becoming lower in value
- Edge of the network is becoming more important
- New services without changes to network (separation of service layer from network layer)
- Complex but longer tail services vs.. Existing simple services with mass demand

Mobile subscribers outnumber Internet users 2 to 1



*Sources: *Nokia; **Morgan Stanley Research and Morgan Stanley Communications Equipment Research.*

NOKIA

Mobile : Now a first class citizen of the web

FUTURETEXT

- Globally, at end of 2005, there were 2.1 billion mobile phones vs. 1.0 billion Internet users.
- Even amongst those one billion Internet users, over 200 million of them accessed the Internet via a mobile phone (mostly in Japan, China and South Korea).

Mobile is now a first class citizen of the Web.
More so, with Web 2.0 (Mobile Web 2.0) -
Voice, SMS, Mobile Web?

Mobile Widgets - Nokia ..

When we extend this definition to ‘Mobile Web 2.0’ – there are two implications :

a) The Web does not necessarily extend to mobile devices

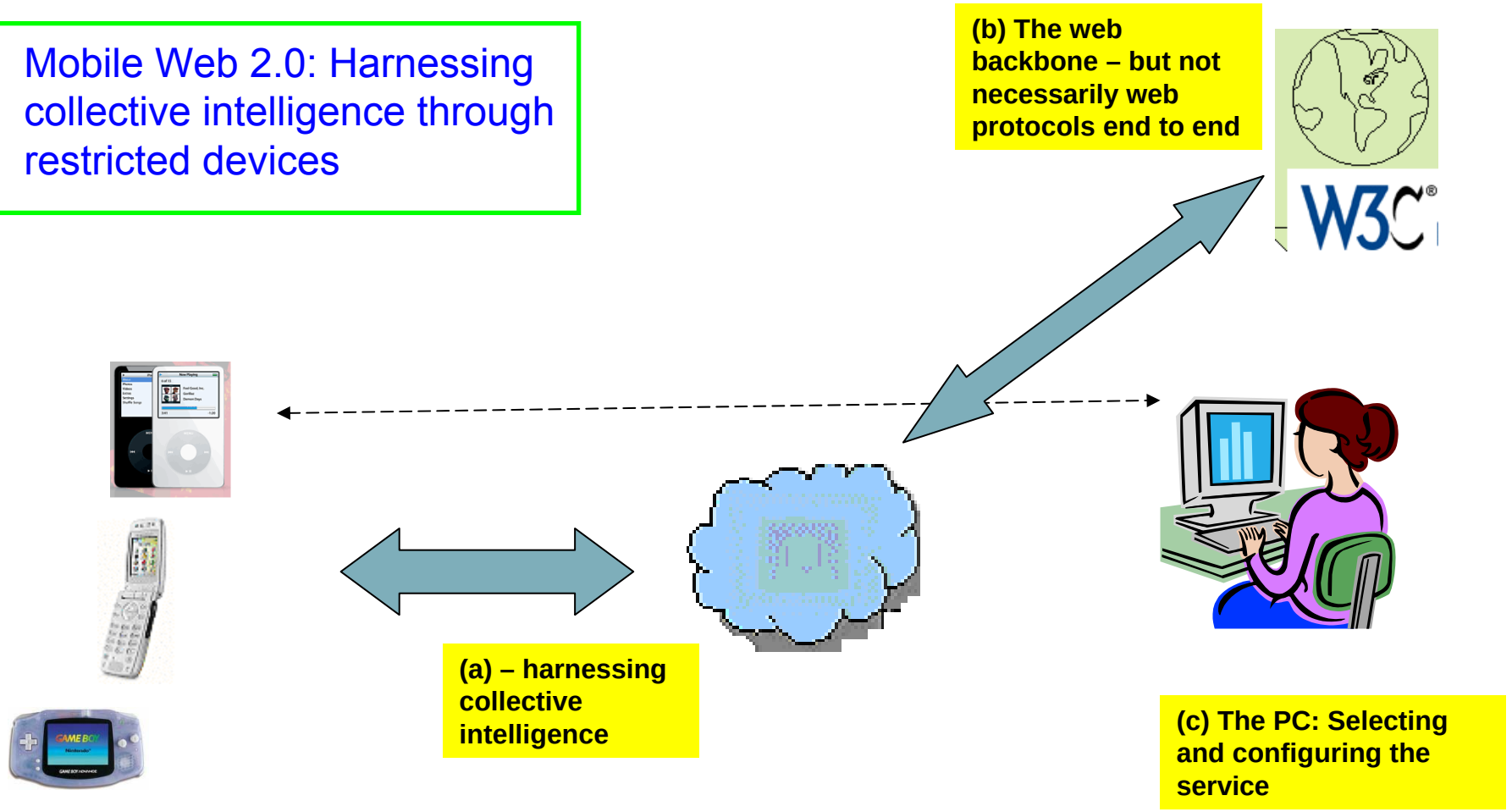
b) Even though the Web does not extend to mobile devices, intelligence can still be captured from mobile devices.

Not ringtones etc (packaged content)!

Mobile Web 2.0 != Packaged content (ringtones)

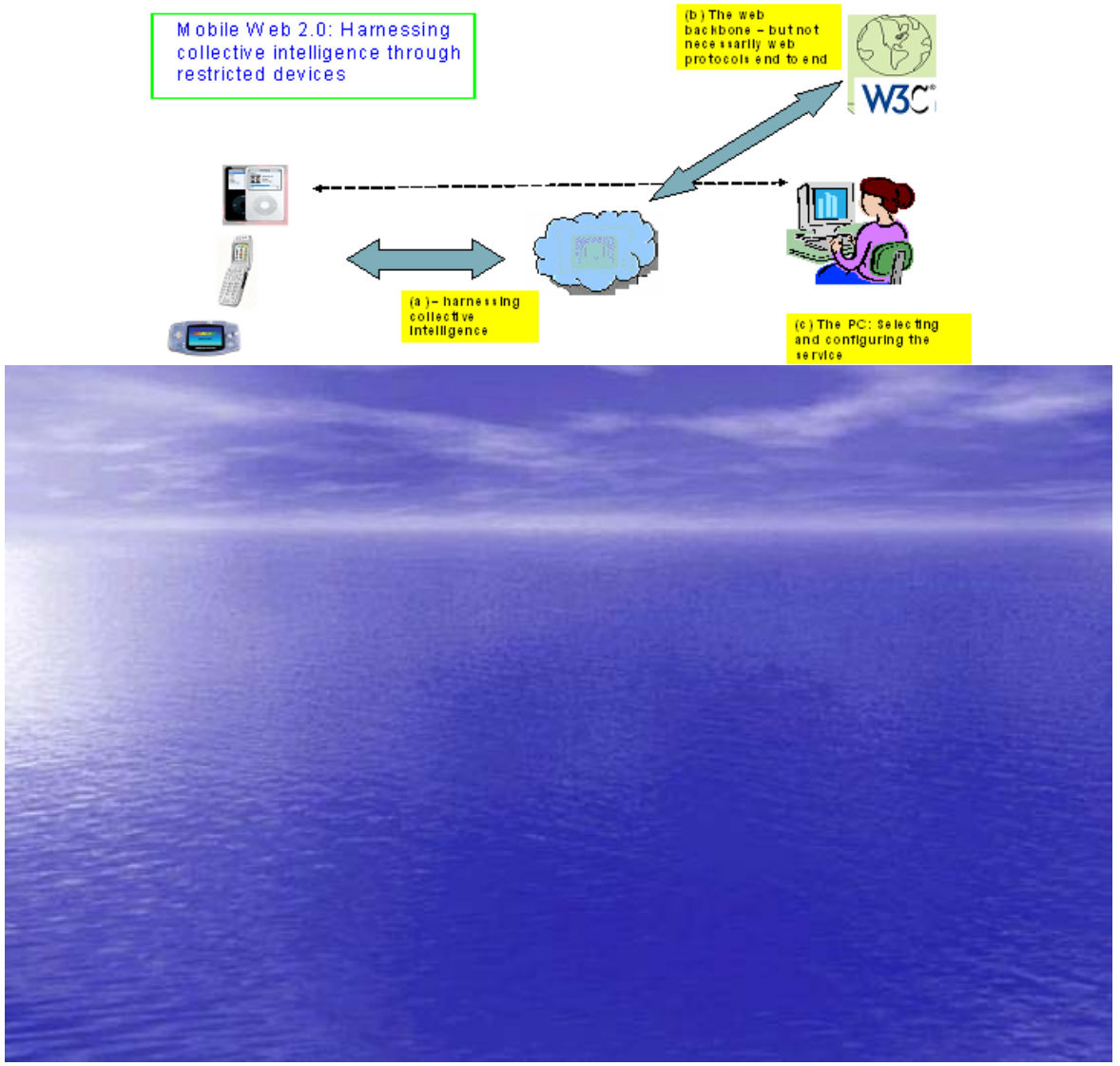
FUTURETEXT

Mobile Web 2.0: Harnessing collective intelligence through restricted devices



The Deep blue sea problem …

FUTURETEXT



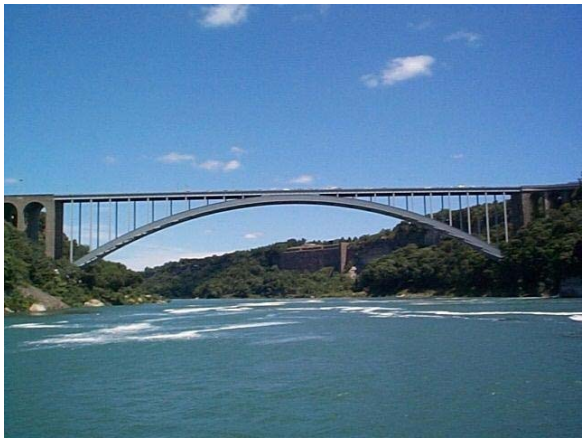
flickr

YouTube
Broadcast Yourself™

facebook

UK myspace
a place for friends

Deep blue sea problem ..



So, the question is: How does the mobile device adopt the ethos of the Web and yet maintain some unique advantages? i.e. bridge the world of the Mobile and the Internet?

At least Eleven ways are possible to implement Mobile Web 2.0 i.e. for mobile to add a unique element to Web 2.0

1) The Operator implementation – This will be likely based on IMS/SDP.

2) **The handset implantation** – This approach is best indicated by Nokia's Ovi strategy and the iPhone.

3) **The Enterprise network strategy** – Best epitomised by Cisco's foray into Web 2.0 based on recent acquisitions such as Tribes and Five Across

4) **The Web players coming to mobile** .. Best example of this approach is Android.

5) **Mobile Web 2.0 and Devices** –Amazon Kindle

6) **SCWS(Smart card web server)** – A relatively new approach with the SIM cards being increasingly powerful and with the deployment of a web server on SIM cards.

7) **Identity and Security** – Identity and Security can complement almost any service and a telecoms network has an advantage there.

8) **Browser APIs/DOM extensions**

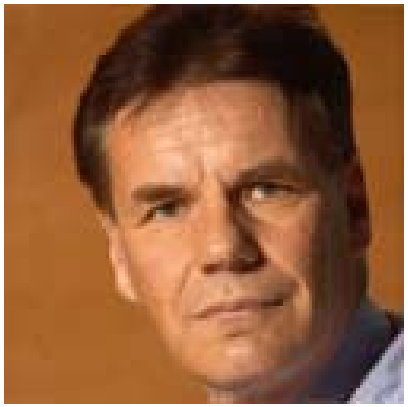
9) **Voice Call detail records** to create social graphs –

10) **Make it quicker / easier** – users will always pay extra for the small improvements which make their life easier even when other(more cumbersome) ways exist which may be cheaper. 11) and finally, there is the concept of Umbrella social networks Beyond Web 2.0

11) **Umbrella social networks**

Mobile Mobile Mobile ..

FUTURETEXT



Mobile Mobile Mobile.. Eric Schmidt - Google

Nokia is going to be an Internet company - Nokia chairman Olli-Pekka Kallasvuo

How can big and small developers get their apps on the iPhone - Steve Jobs - Apple

Social networking – the Basics

Philosophy

People are sharing more – esp personal information.(ex Twitter)

In an era of commoditization, people are looking to express themselves ..

What is the difference between a song and a ringtone: A song is something you consume vs. ringtone is something you display. Hence ringtone has ‘more’ value than the song even when it is a poor copy of the song

As computers become commoditised .. people buy the Apple for what it means!(and less for what it does) – i.e. a means of expression

Social software, social media, social networking are the drivers behind Web 2.0

What does social networking comprise of?

FUTURETEXT

- Web based online communities
- A user profile
- Links to ‘friends’
- Groups (open or closed)
- Free to join and use
- Blogging
- Sharing of multimedia contact (video, pictures etc)
- Around an object or around a person

Social maintenance

Self expression

Distraction!

Other social trends:

Byproduct of social life, Geography, Friends who never meet, Online dating

Social maintenance ..

FUTURETEXT

1) Keeping in contact with friends & family

2) Making new friends Arranging social life,

3) Kept in touch 24/7

4) Larger more complex friendship groups

5) Background chat to maintain relationships & co-presence,

6) Awareness of movements & mood of others

7) Asynchronous communications through wall postings & news feeds
text & MSN & email...

FUTURETEXT

Before mobile

8) Face to face encounters then more face to face or not!

9) With mobile & MSN

10) Text and MSN safe media for getting to know people

11) People began to meet friends online through other friends

FUTURETEXT

With social networking

12) Collecting friends part of social networking culture

13) Show relationship status online

14) Concerns about inappropriate disclosure of phone numbers & addresses

15) No firm plans (timewise)

Self expression ...

FUTURETEXT

1) Phone covers, ring tones, user names, profile decorations, second life profiles

2) In group humour supported by text

3) Group banter on MSN

4) Profile

5) listing of interests

6) Blogging

7) Writing on friends walls

8) Join groups

9) Sharing interests by posting comments

10) flash mobbing and record breaking (impromptu raves)

Distraction ..

FUTURETEXT

1) Snake!

2) Lecture based texting

3) MSN – an addictive distraction

4) Reading other peoples walls, adding friends,

5) Viewing & tagging photos

6) Creating lists

7) Joining groups

FUTURETEXT

More contacts

- Lower effort than MSN & text to maintain existing friends
- Low risk way of making new friends
- New way of finding friends in common

More distraction

- Another reason not to work!

Greater self expression

Less privacy

- Inappropriate display of personal information
- Inappropriate posting of photos & video

Principles of Web 2.0 ..

What is Web 2.0

a) Web as a platform:
pets.com TV (v.s. Google)
A web of mainframes?
Connecting the farmer in Africa to the rest of the world.

b) Harnessing collective intelligence : Google page rank

The platform is the Internet,
On the Internet, the rules are different.
Information sharing is actually better than information hoarding.

With enough people sharing information – you build a database and the database becomes bigger and better with incremental users

Business models

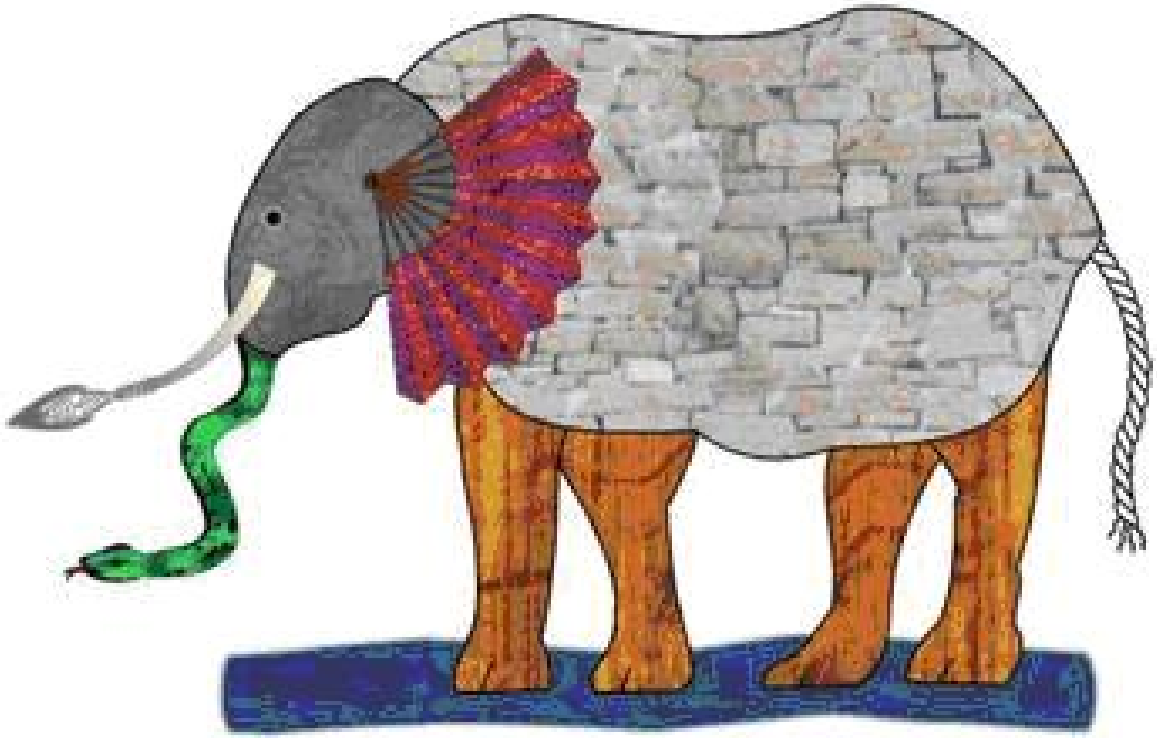
User enhanced databases - Amazon reviews

On the Internet, you build a product that gets better as you harness the intelligence of the users. Hence, users must contribute.

Amazon is a commodity business on one hand (you can't get more commodity than selling books!) but has implemented many small

Web 2.0 innovations (like reviews) so that they are far away from the commodity.

Web 2.0 is all about building systems that get better the more people use them



Like the parable of the blind men and the elephant, many see only one aspect of Web 2.0, but miss the big picture

Image source: http://www.wordfocus.com/word-act-blindmen.html

What is Web 2.0

a) Web as a platform:
pets.com TV (v.s. Google)
A web of mainframes?
Connecting the farmer in Africa to the rest of the world.

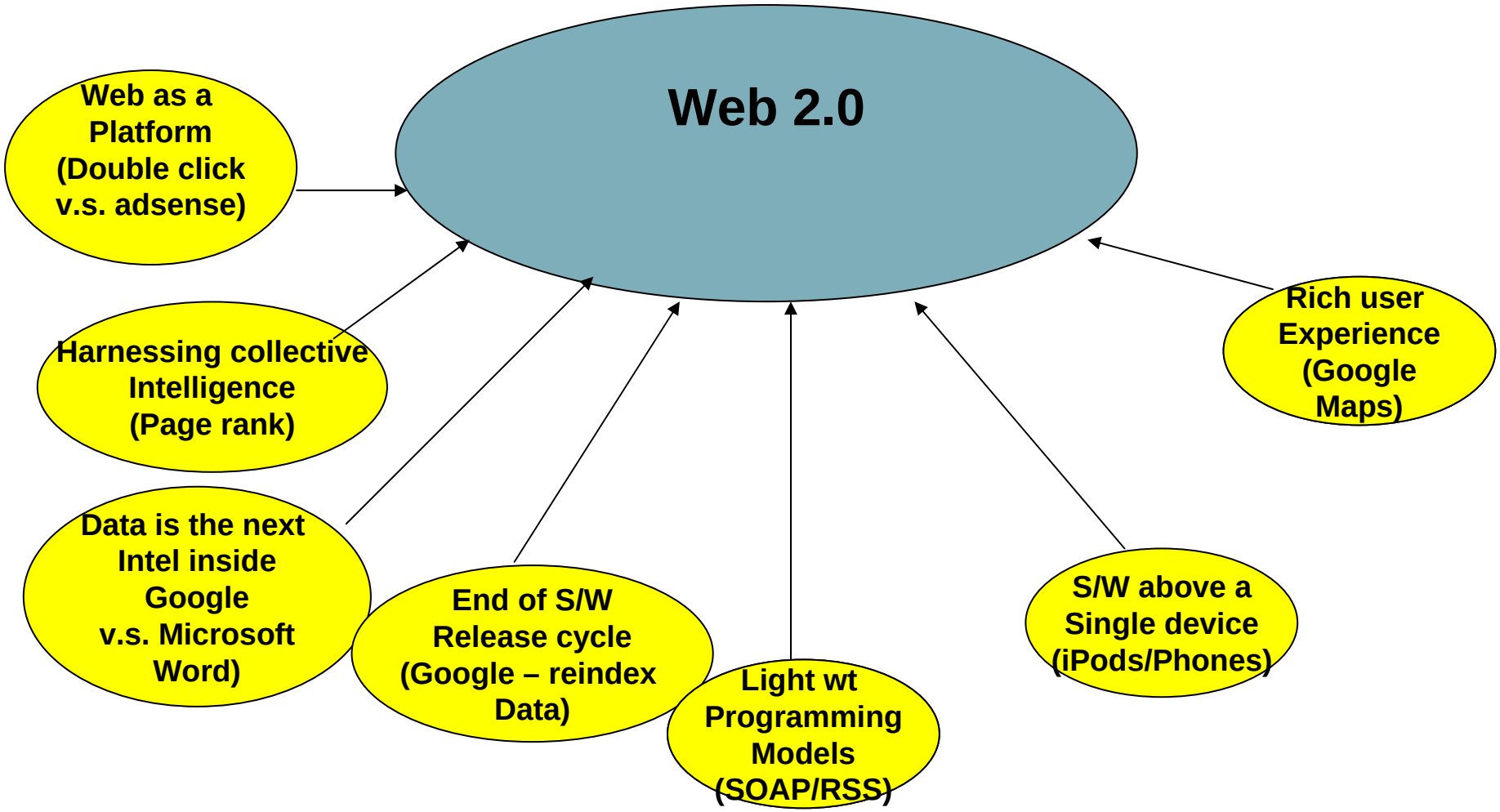
b) Harnessing collective intelligence : Google page rank

The platform is the Internet,
On the Internet, the rules are different.
Information sharing is actually better than information hoarding.

With enough people sharing information – you build a database and the database becomes bigger and better with incremental users

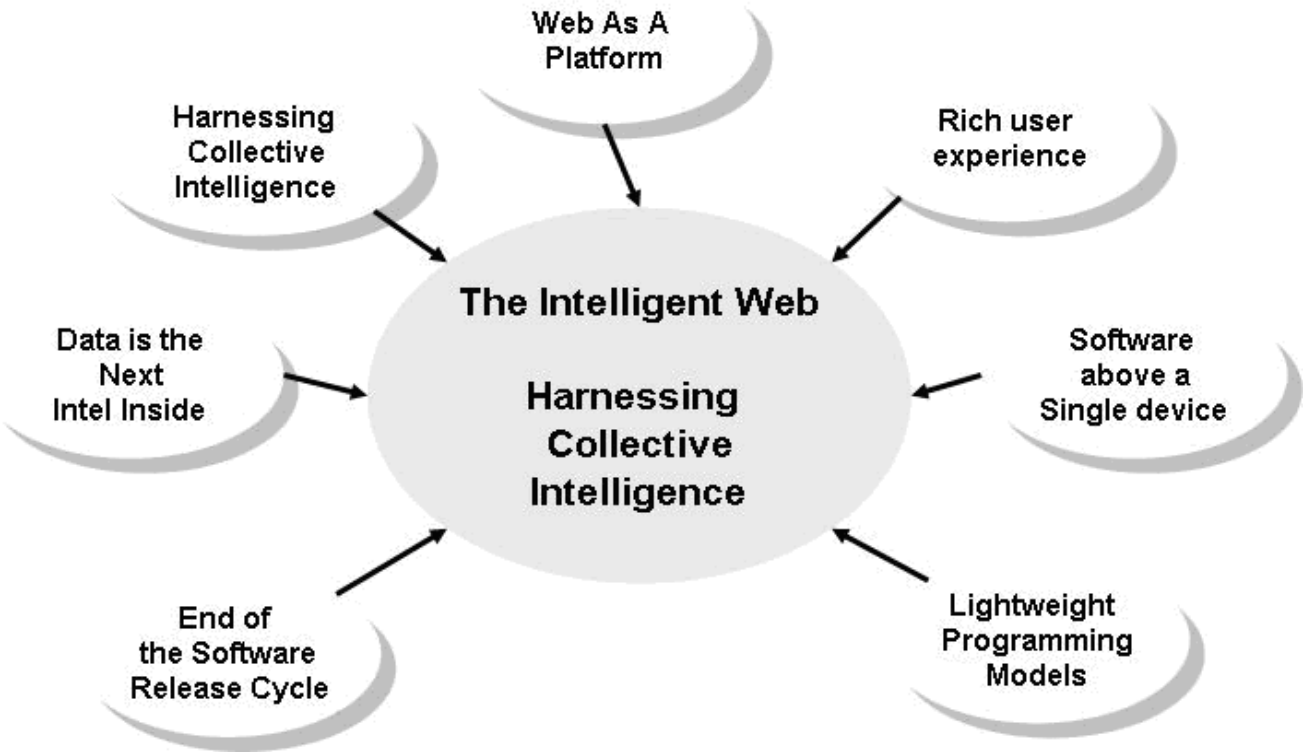
Web 2.0: The seven principles

FUTURETEXT



http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html

FUTURETEXT



Was featured on the O Reilly radar : April 2006 (All other principles feed into the second principle http://radar.oreilly.com/archives/2006/04/principles_of_web_20_make_more.html

Harnessing collective intelligence is a complex process. There are at least five ways to harness collective intelligence (Dion Hinchcliffe)

1) Be the Hub of a Hard to Recreate Data Source – ex wikipedia

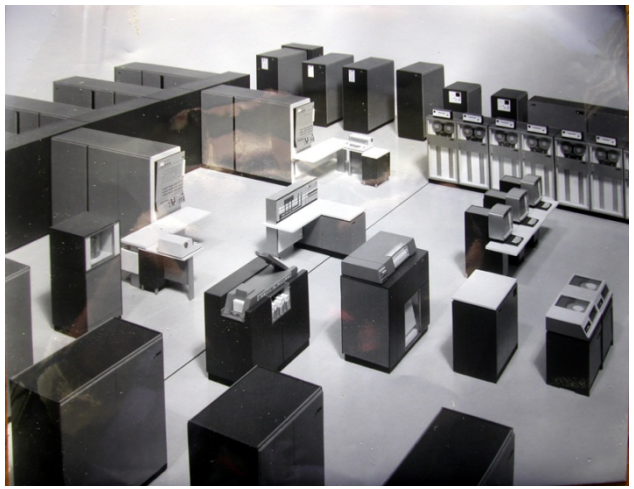
2) Seek Collective Intelligence out – Google

3) Trigger Large-Scale Network Effects - Katrinalist and CivicSpace (http://en.wikipedia.org/wiki/CivicSpace (Howard Dean's political campaign)

4) Provide A Folksonomy - Self-organization Flickr and del.icio.us .

5) Create a Reverse Intelligence Filter - Memorandum have been using this to great effect. The idea is that hyperlinks, trackbacks, and other information references can be counted and used as a reference to determine what it's important. (Digg)

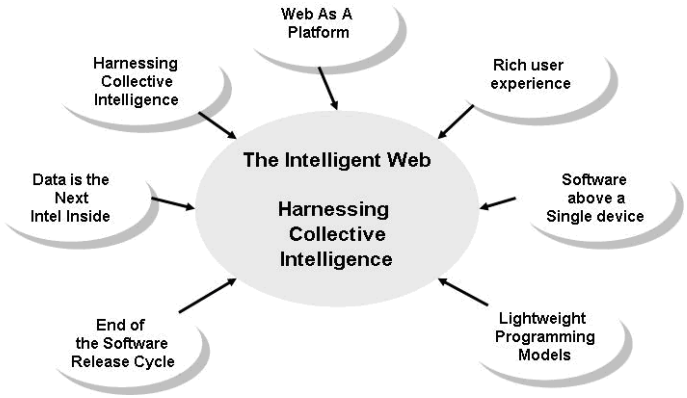
Web as a platform: The Web / Open standards is the only true global unifying force - you can't build a 'Web' out of mainframes - powerful as they are!



http://www.staff.ncl.ac.uk/roger.broughton/firmware/mainframe.htm

FUTURETEXT

Harnessing Collective Intelligence: Now becomes the 'main' principle.

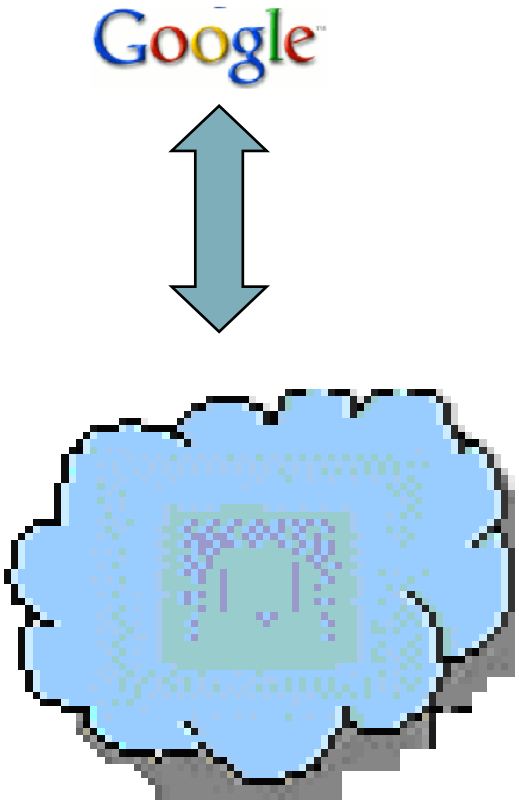


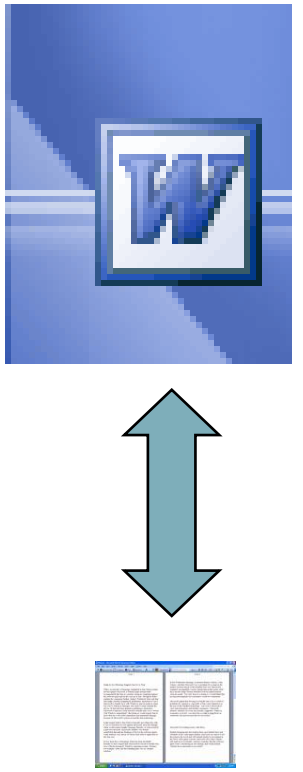
Think page rank:

Global, Web based, Billions of individual contributions (information about web pages), Algorithm, Derived information commercially valuable

FUTURETEXT

Data is the next 'Intel Inside'





End of the software release cycle

Google 95

Google 97

Google 2000

Google 2003

Google 2007

Makes no sense does it!!

Lightweight programming models ..

The heavy weight programming models catered for the few. In contrast, using lightweight programming models we can reach many more people (hence sources of information – to enable data collection and a more intelligent web).

For example: Amazon.com's web services are provided in two forms: The more complex SOAP (Simple Object Access Protocol) web services stack and the simpler REST (Representational State Transfer) stack. (REST is essentially providing XML data over HTTP)

The SOAP stack is used by high value B2B connections (like those between Amazon and retail partners like ToysRUs).
However, 95% of the usage is of the lightweight REST service.

Software above a single device ..

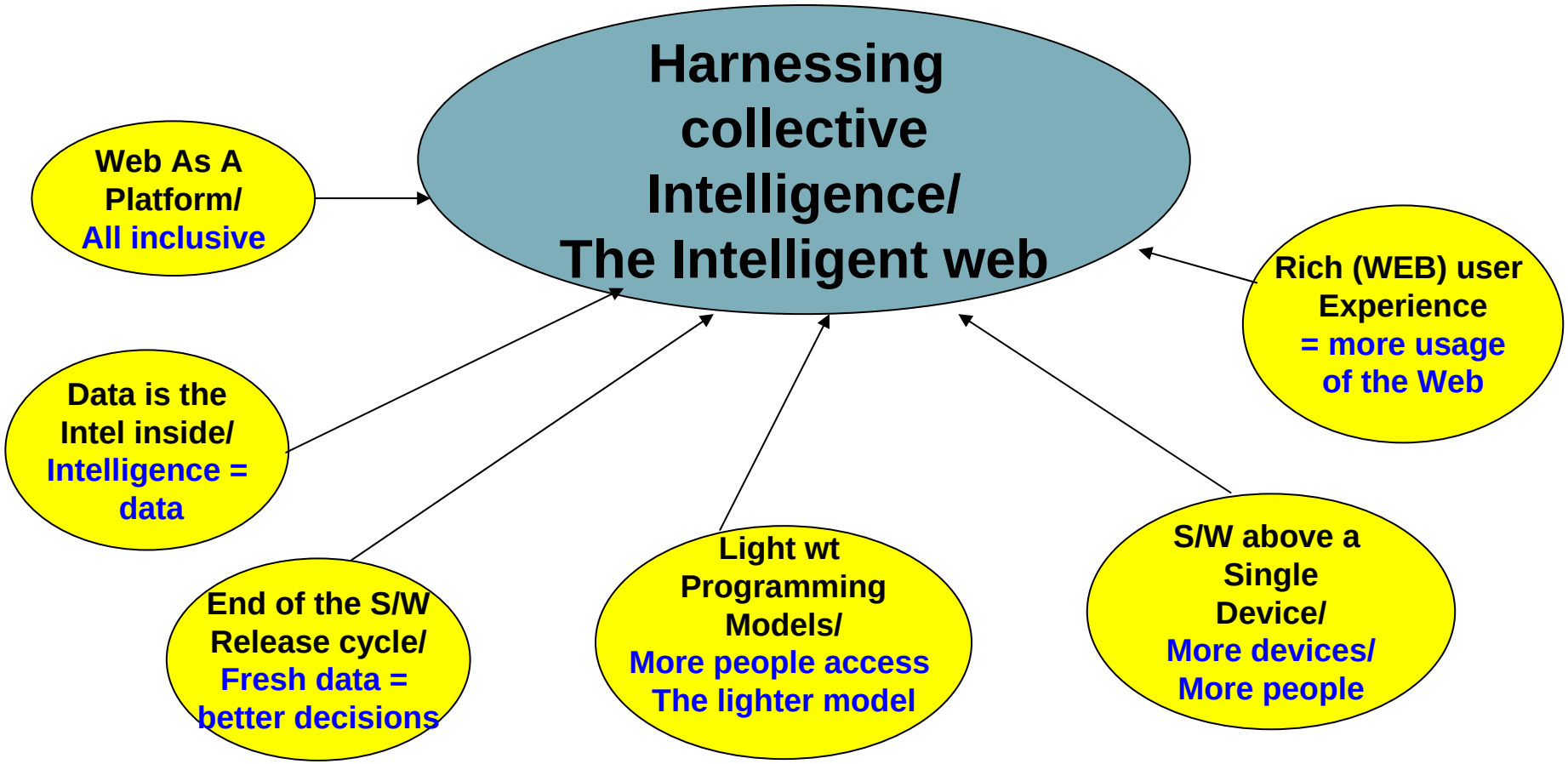
In a word: Mobile Web 2.0!!

Rich user experience ..

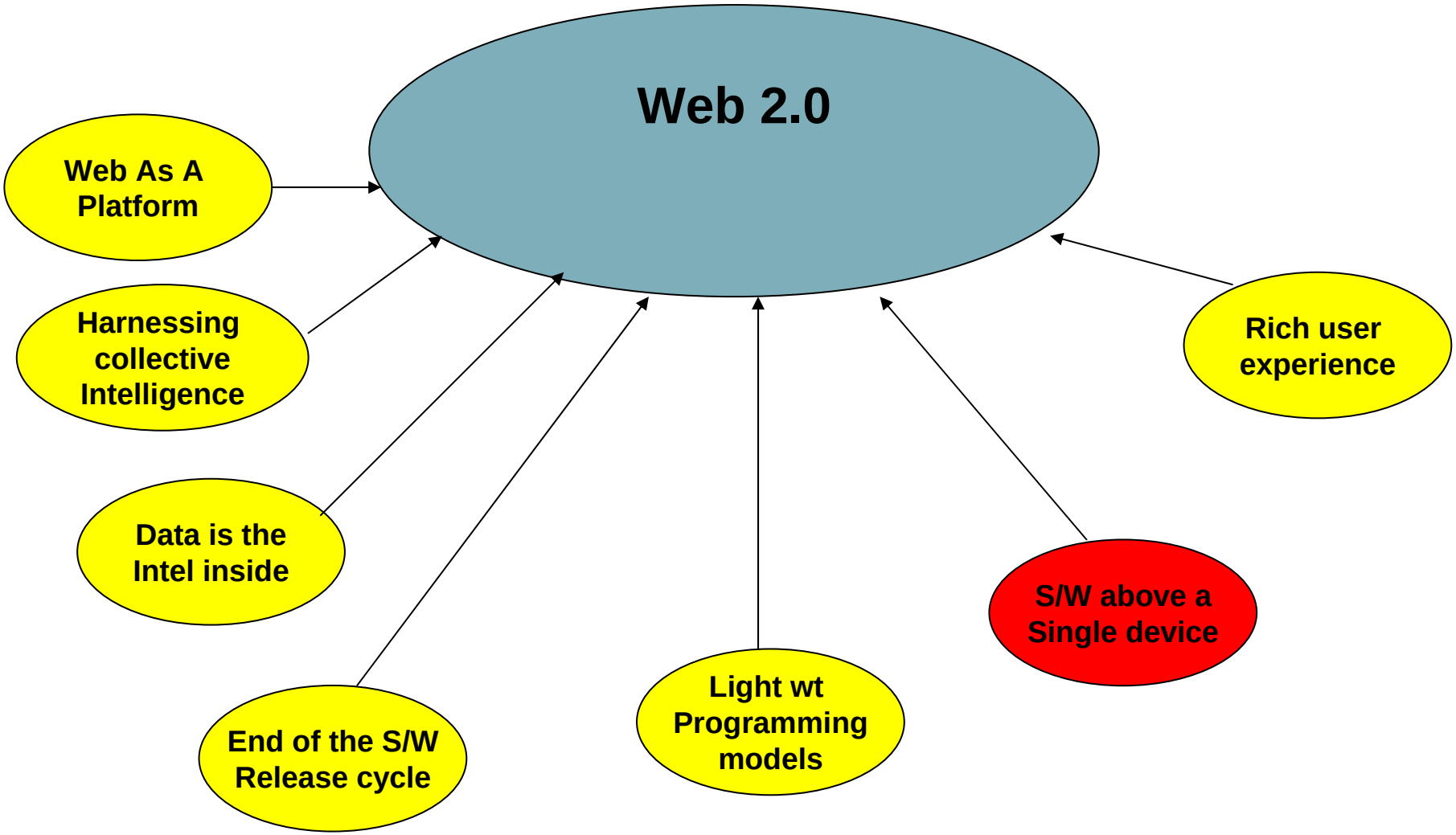
Desktop like UI - best exemplified by Ajax but also Adobe Flex and others

A rich user experience is necessary to enable better web applications leading to more web usage and better information flow on the web - leading of course to a more 'Intelligent' web.

FUTURETEXT



Was featured on the O Reilly radar : April 2006 (All other principles feed into the second principle http://radar.oreilly.com/archives/2006/04/principles_of_web_20_make_more.html



Questions?

FUTURETEXT

Questions?

FUTURETEXT

http://www.youtube.com/watch?v=6a_KF7TYKVc&feature=related social networking In plain english
http://www.youtube.com/watch?v=MpIOClX1jPE&feature=user social media in plain english]
http://www.youtube.com/watch?v=y-MSL42NV3c&feature=user podcasting in planin english
http://www.youtube.com/watch?v=-dnL00TdmLY&feature=user wikis inplain english
http://www.youtube.com/watch?v=NN2I1pWXjXI&feature=user Blogs in plain english
http://www.youtube.com/watch?v=x66lV7GOcNU&feature=user social book marking in plain english

Mobile Web 2.0 – Significance and unique elements

When we extend this definition to ‘Mobile Web 2.0’ – there are two implications :

a) The Web does not necessarily extend to mobile devices

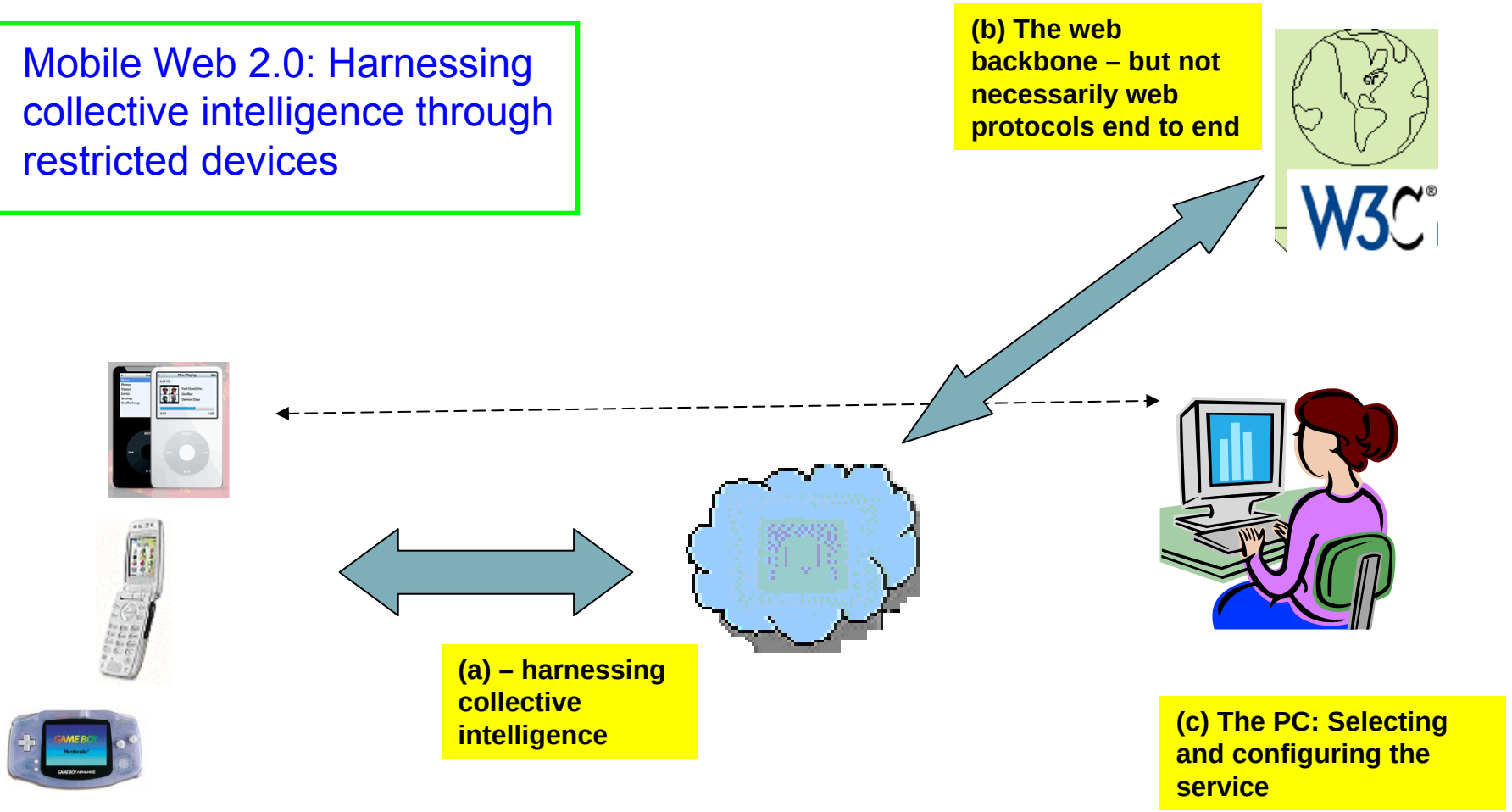
b) Even though the Web does not extend to mobile devices, intelligence can still be captured from mobile devices.

Not ringtones etc (packaged content)!

Mobile Web 2.0 != Packaged content (ringtones)

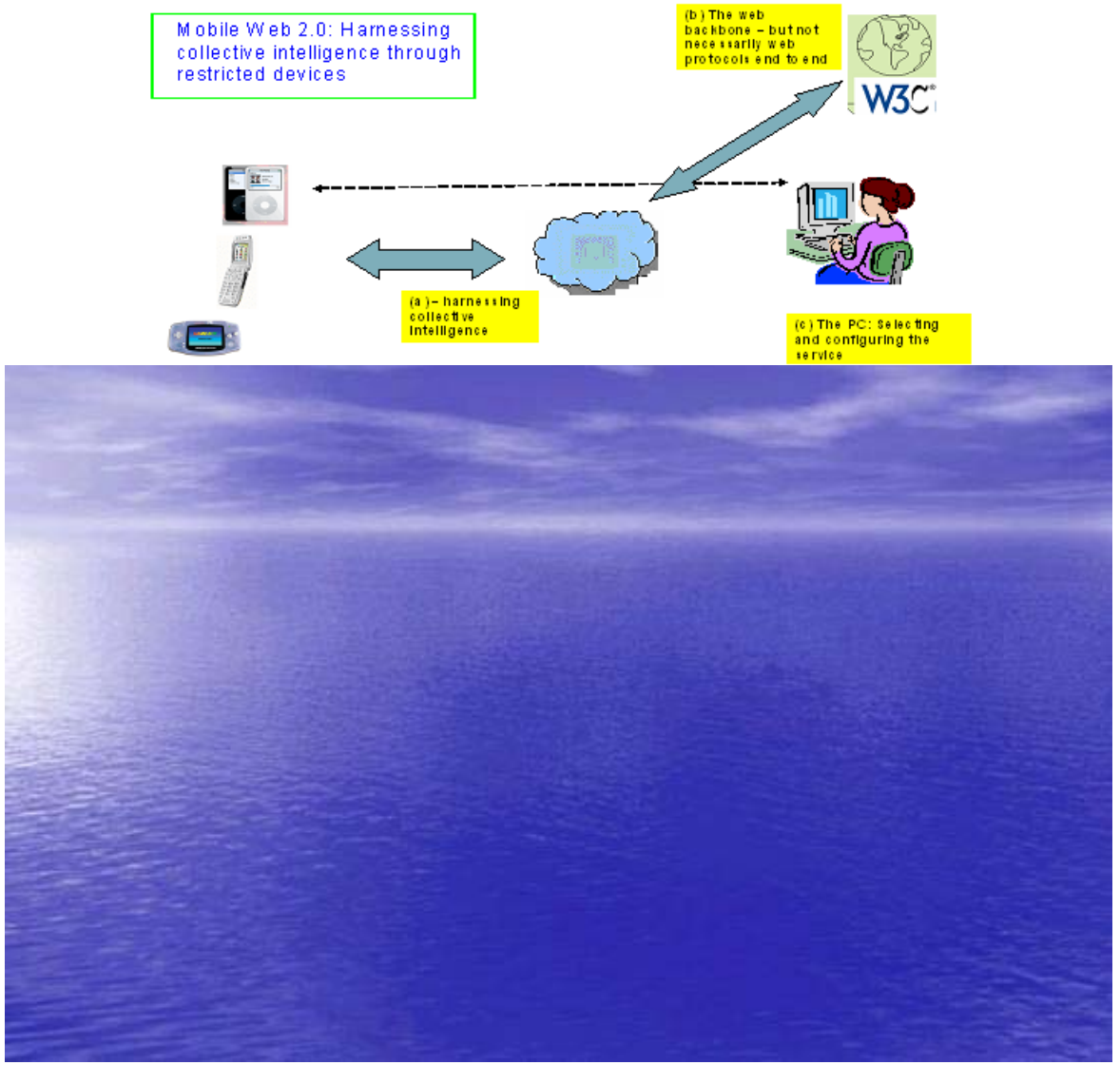
FUTURETEXT

Mobile Web 2.0: Harnessing collective intelligence through restricted devices



The Deep blue sea problem …

FUTURETEXT



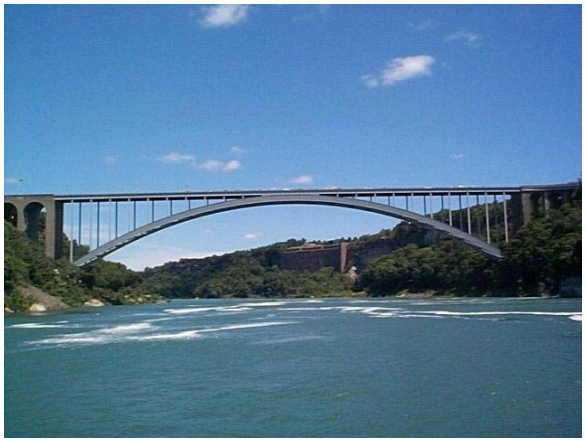
flickr

YouTube
Broadcast Yourself™

facebook

UK myspace
a place for friends

Deep blue sea problem ..



So, the question is: How does the mobile device adopt the ethos of the Web and yet maintain some unique advantages? i.e. bridge the world of the Mobile and the Internet?

At least Eleven ways are possible to implement Mobile Web 2.0 i.e. for mobile to add a unique element to Web 2.0

1) The Operator implementation – This will be likely based on IMS/SDP.

2) **The handset implantation** – This approach is best indicated by Nokia's Ovi strategy and the iPhone.

3) **The Enterprise network strategy** – Best epitomised by Cisco's foray into Web 2.0 based on recent acquisitions such as Tribes and Five Across

4) **The Web players coming to mobile** .. Best example of this approach is Android.

5) **Mobile Web 2.0 and Devices** –Amazon Kindle

6) **SCWS(Smart card web server)** – A relatively new approach with the SIM cards being increasingly powerful and with the deployment of a web server on SIM cards.

7) **Identity and Security** – Identity and Security can complement almost any service and a telecoms network has an advantage there.

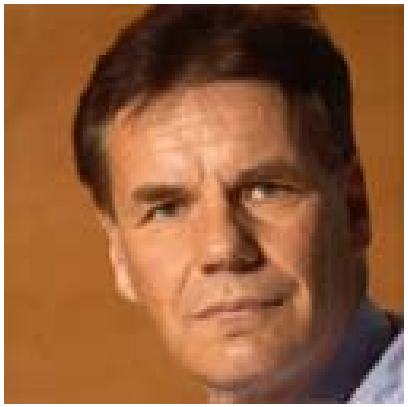
8) **Browser APIs / DOM extensions**

9) **Voice Call detail records** to create social graphs –

10) **Make it quicker / easier** – users will always pay extra for the small improvements which make their life easier even when other(more cumbersome) ways exist which may be cheaper. 11) and finally, there is the concept of Umbrella social networks Beyond Web 2.0

11) **Umbrella social networks**

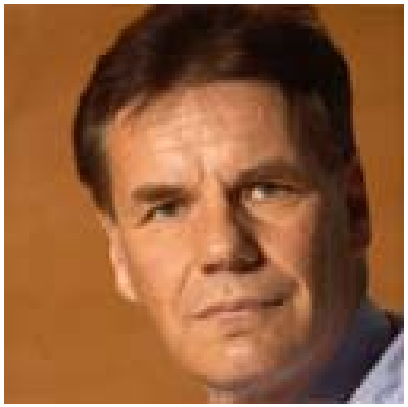
FUTURETEXT



Mobile Mobile Mobile.. Eric Schmidt - Google

Nokia is going to be an Internet company - Nokia chairman Olli-Pekka Kallasvuo

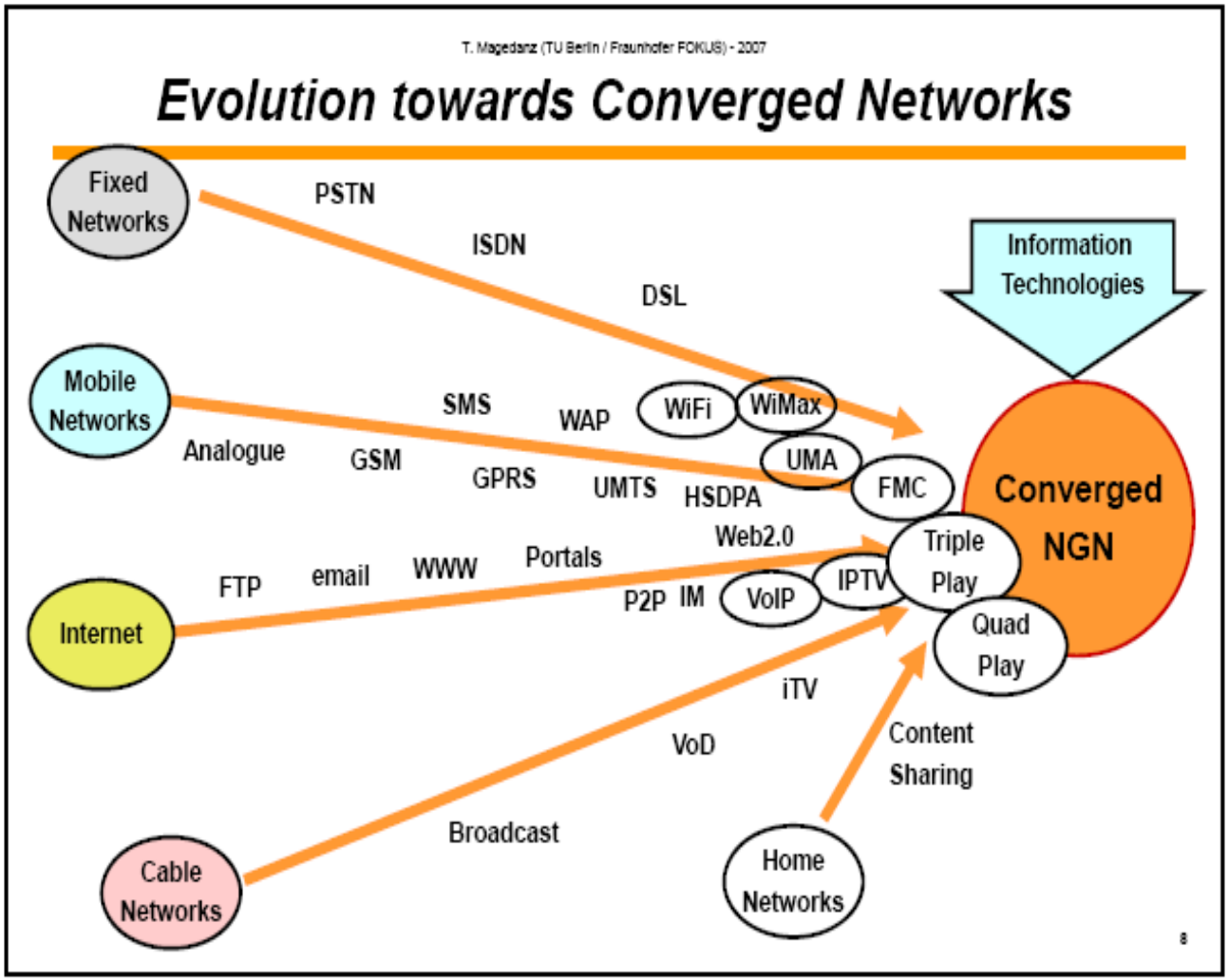
How can big and small developers get their apps on the iPhone - Steve Jobs - Apple



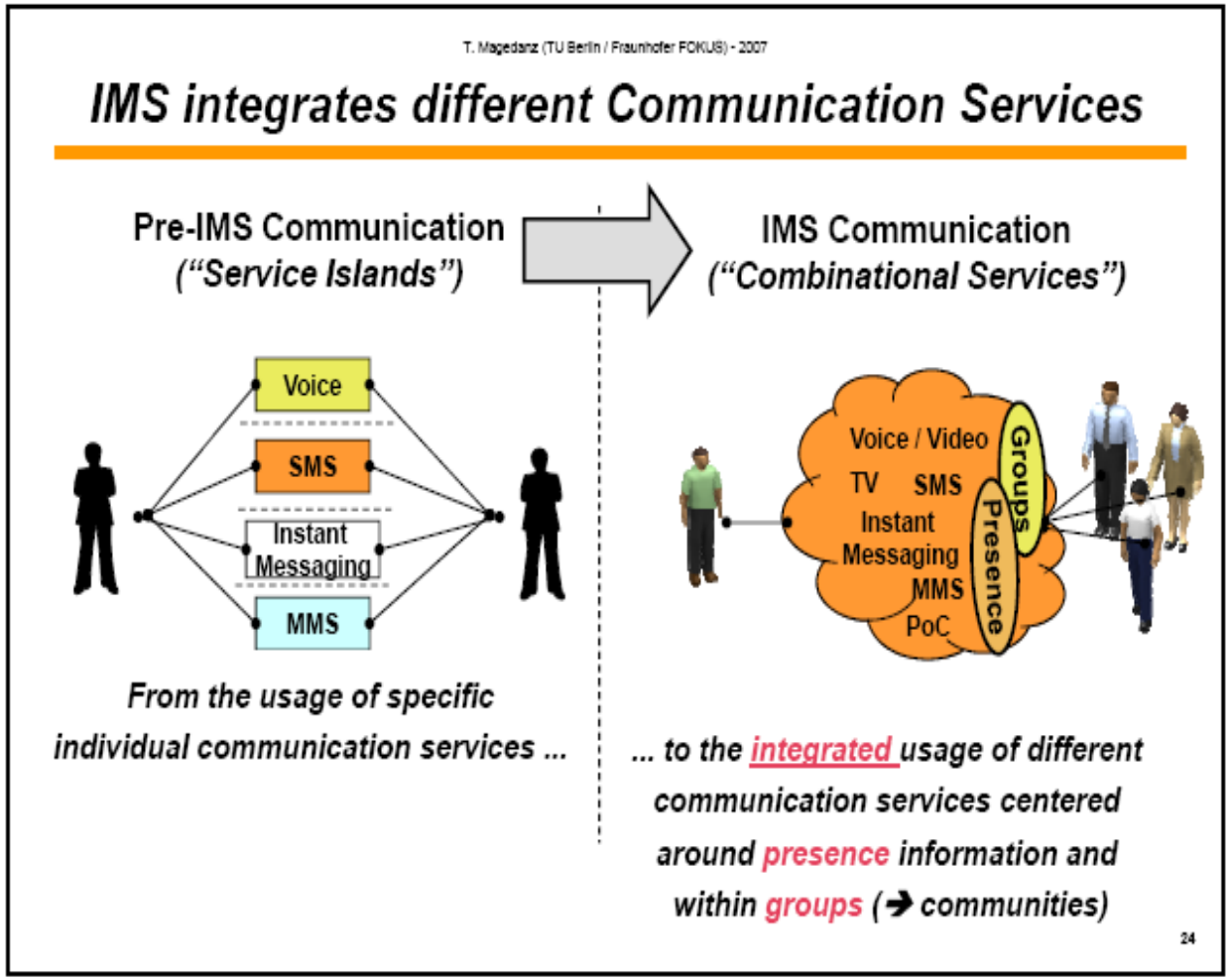
Why is Mobile Web 2.0 important?

iPhone, Android, Nokia are looking at the Web and the Mobile Web together ..

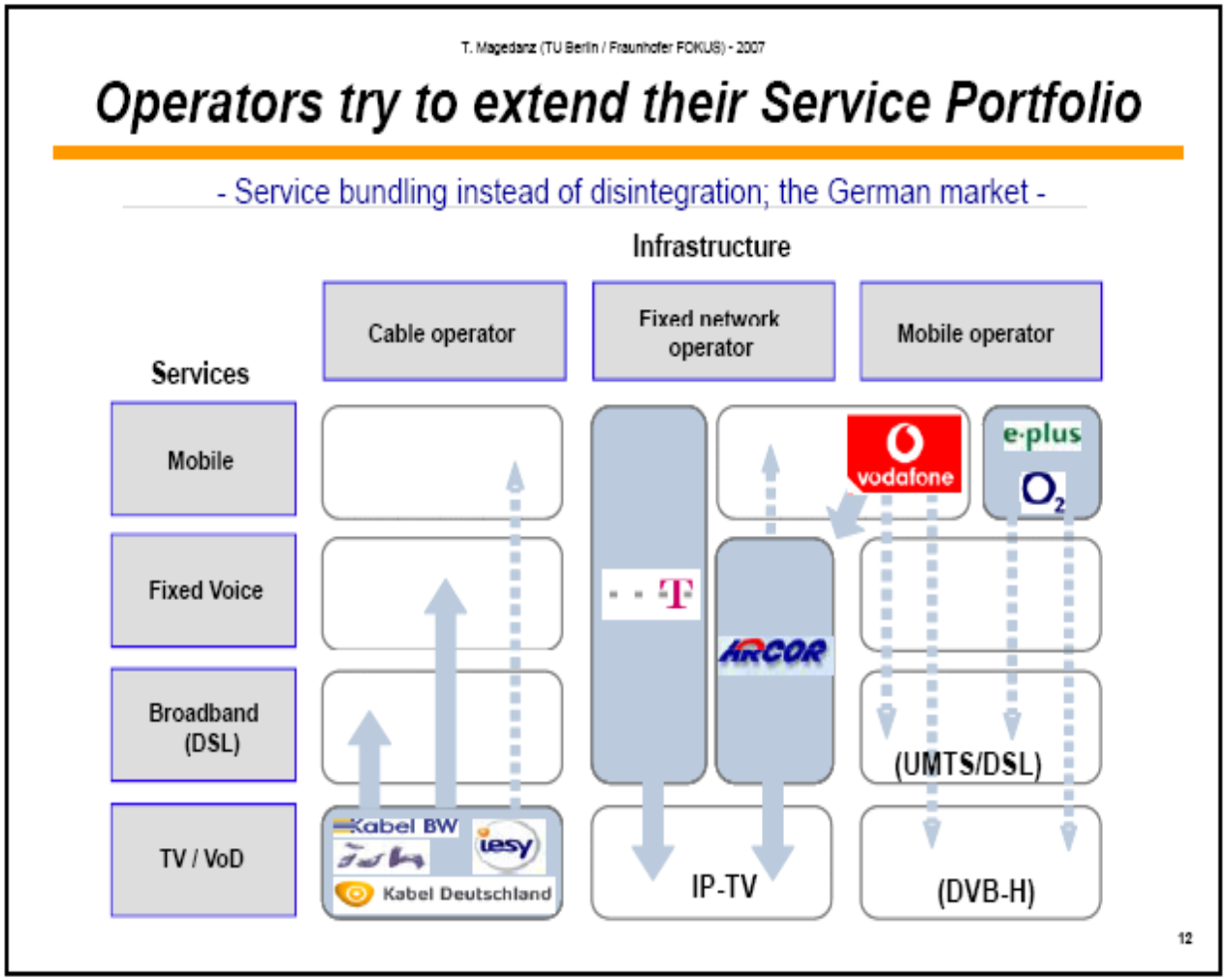
The telco implementation: Based on IMS



Source: Fraunhofer FOKUS



Source: Fraunhofer FOKUS

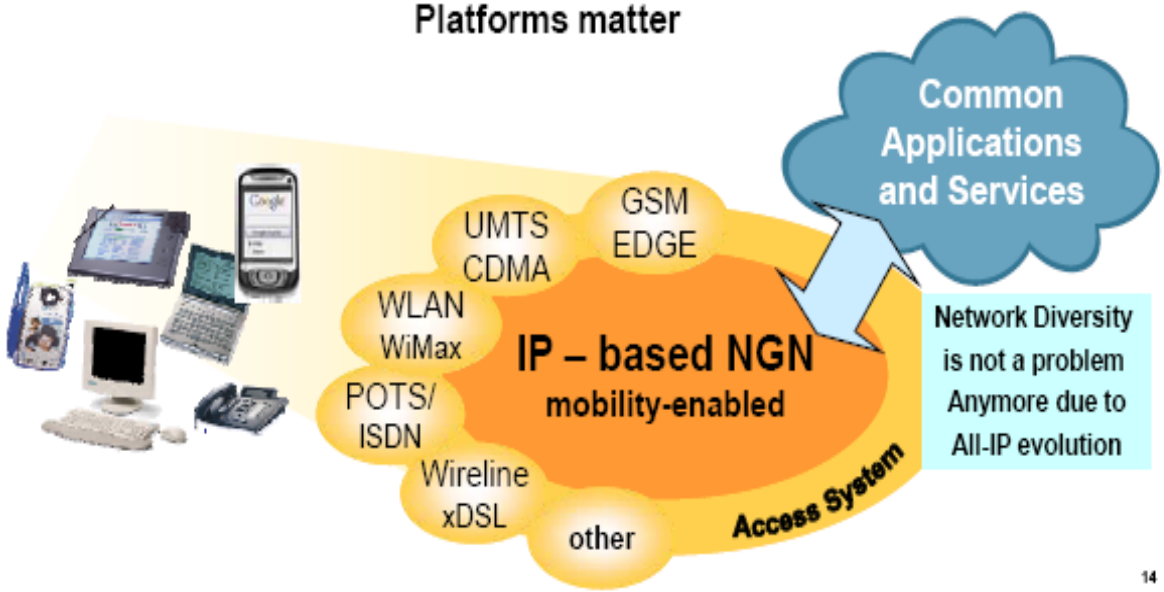


Source: Fraunhofer FOKUS

T. Magedanz (TU Berlin / Fraunhofer FOKUS) - 2007

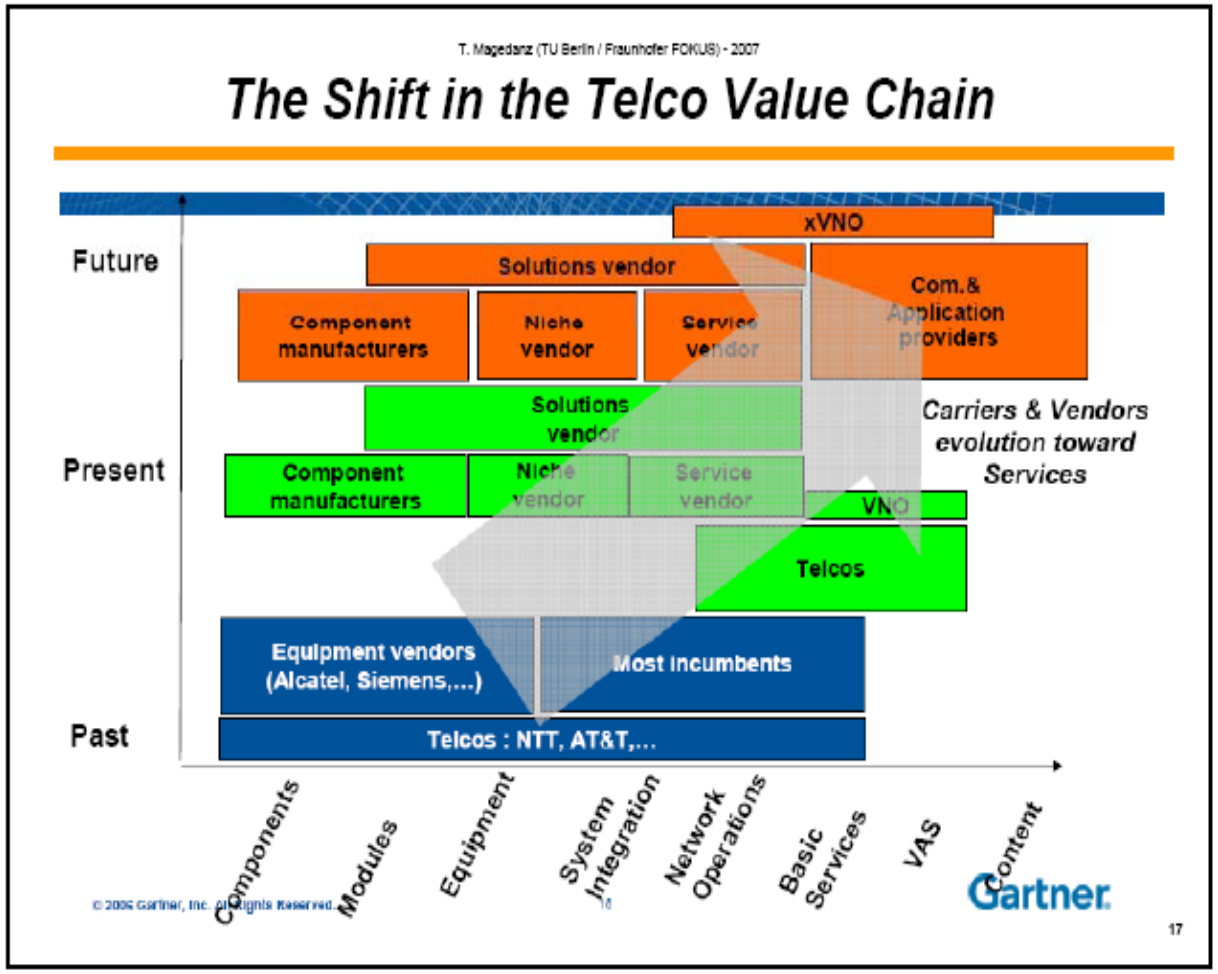
Seamless Services – The Net doesn't Matter

- Network diversity and network innovation pace has lead to network abstraction based on IP as common denominator
  - Connectivity Services versus Multimedia Services
- Users are interested in services – thus end systems and Service Platforms matter

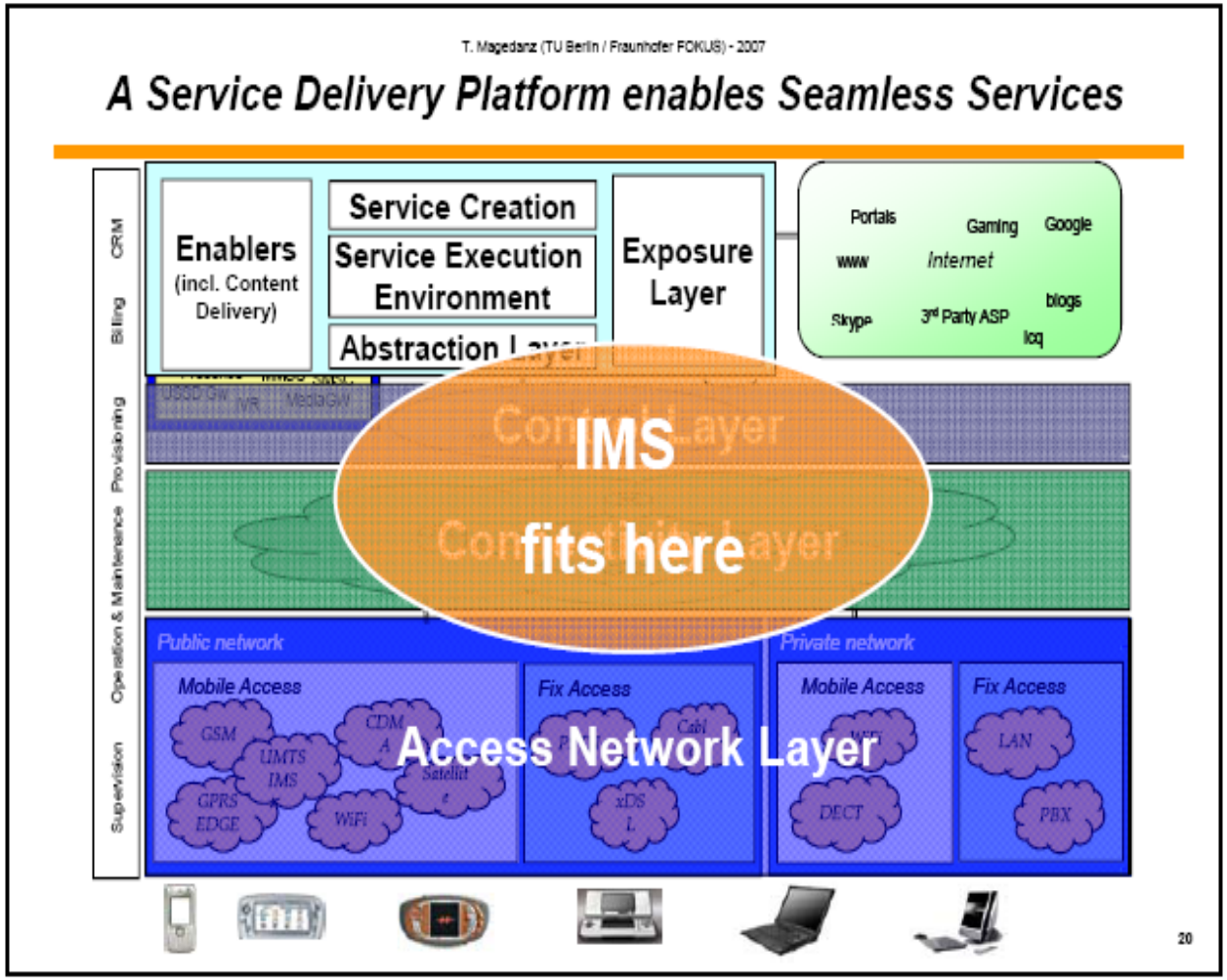


14

Source: Fraunhofer FOKUS



Source: Fraunhofer FOKUS



Source: Fraunhofer FOKUS

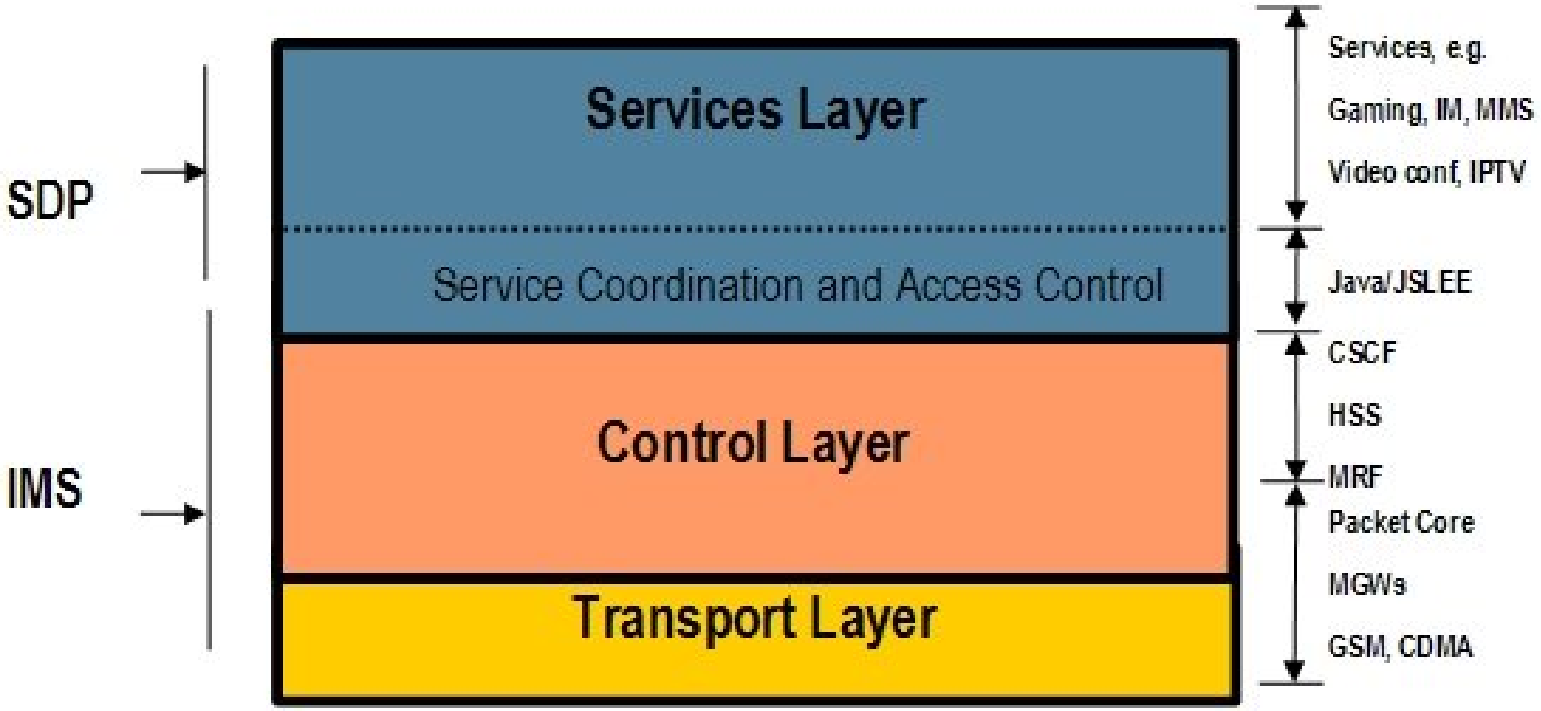


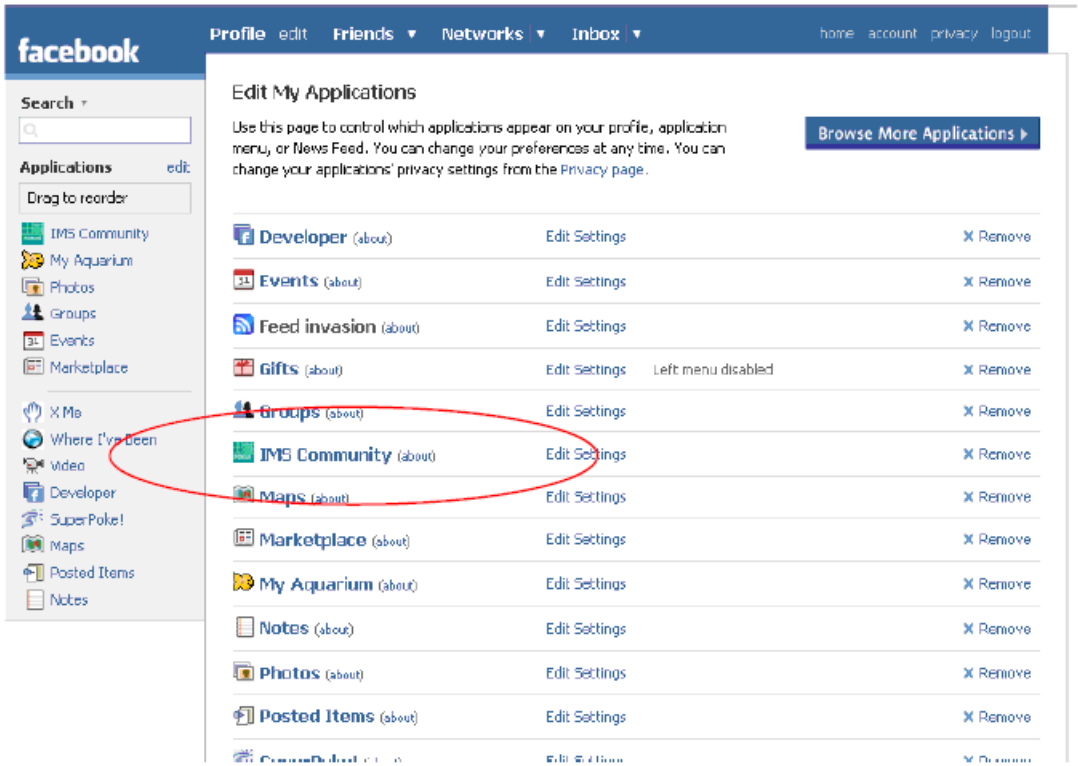
Figure 1.

Source: IMS insider

IMS - SERVICE ENABLERS - SDP

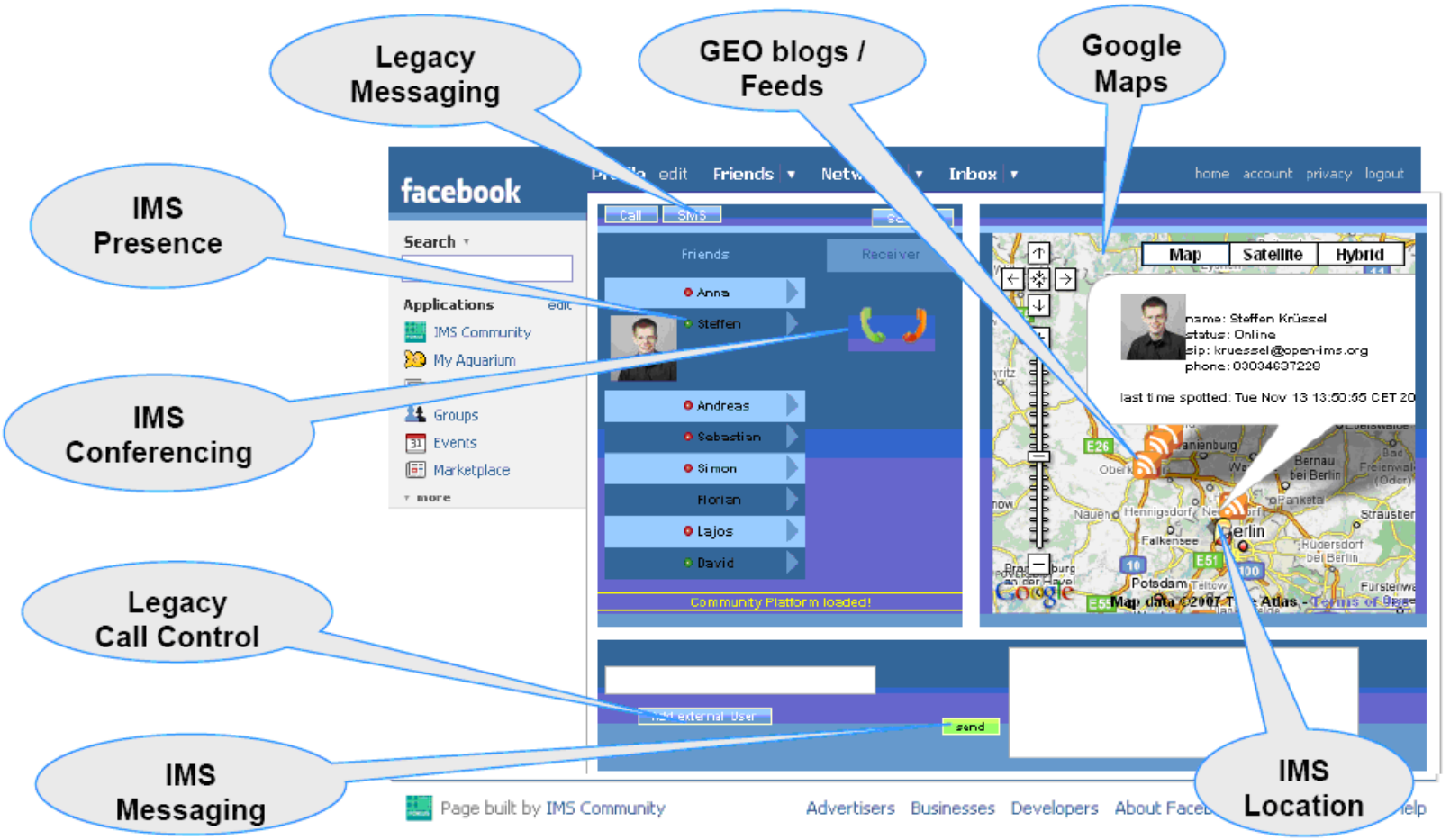
Facebook concept of 3rd party applications

- Possibility to add your own applications to application repository
- Applications can be distributed to specific user profiles
- Specific facebook API for 3rd party service developers using REST and FBML
- IMS Community App to enable facebook users with telco features

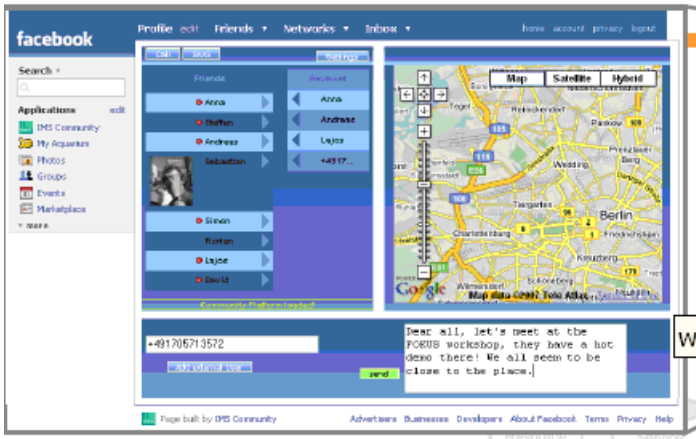


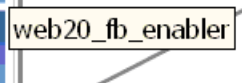
Source: Facebook apps integration - Fraunhofer FOKUS

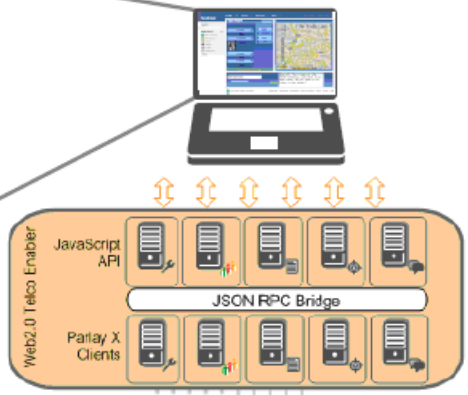
FOKUS Community Facebook Application



FOKUS Web 2.0 Telco Enabler



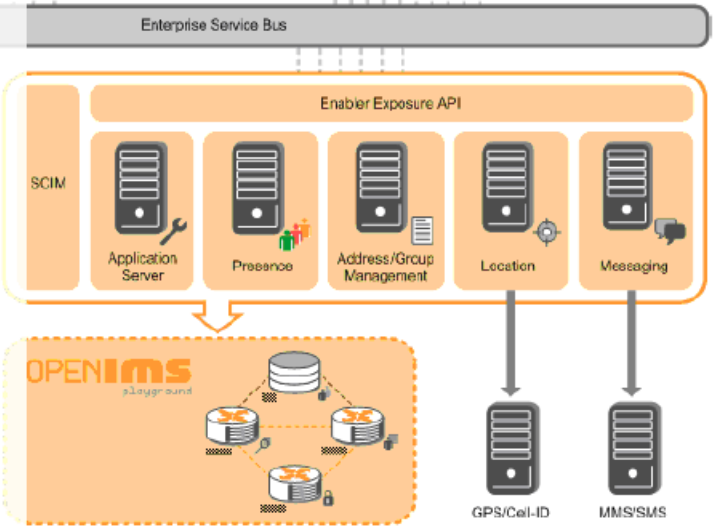




Web 2.0 / Telco Enabler:

- MMS / SIP Instant Messaging
- SMS legacy messaging
- Conferencing
- Location
- Rich Presence

JSON RPC allows easy integration into AJAX-based applications.



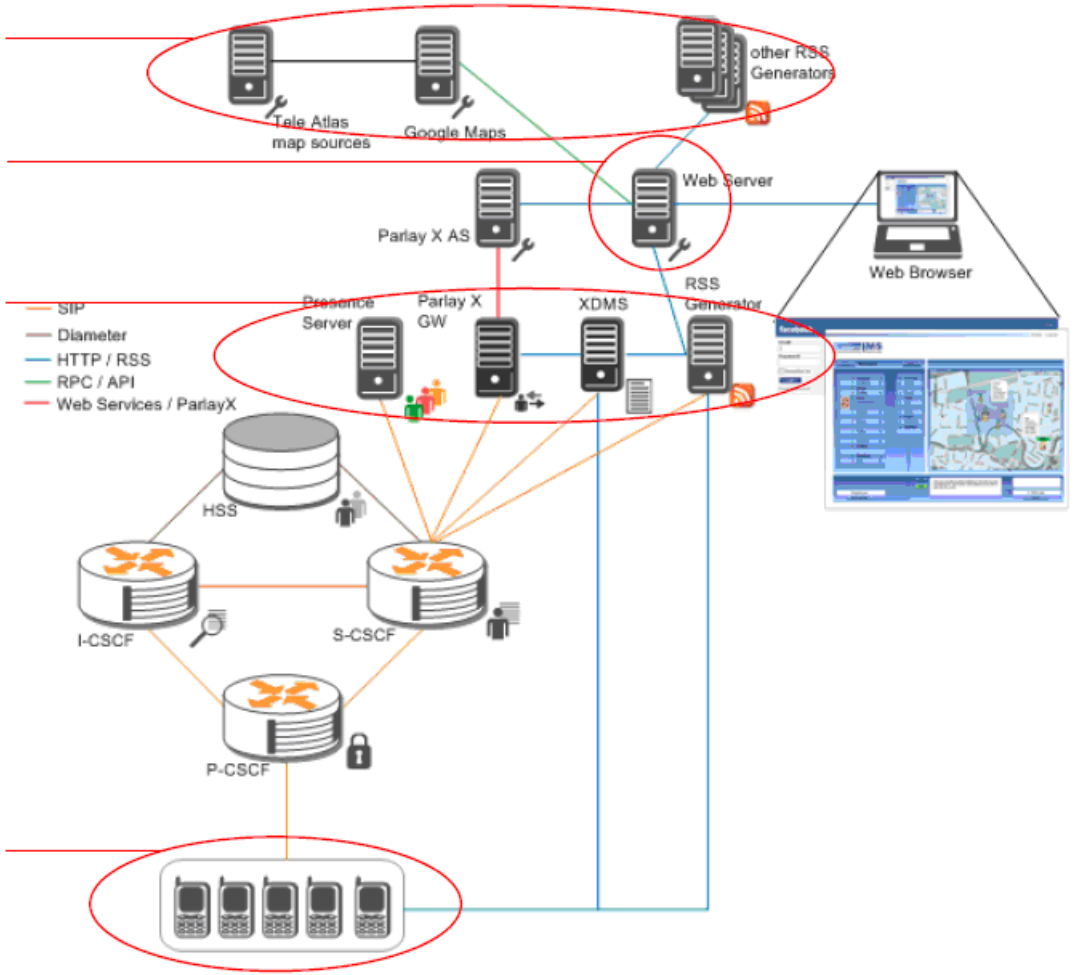
Mashup Architecture

3rd party Web 2.0 enabler

Central mashup node

Telco enabler layer

Telco enabled IMS/Web2.0 clients



13

The Enterprise implementation: Video, collaboration, convergence

Definitions ..

"Unified Communications is the integration of communication and collaboration technologies with business applications and processes in order to improve those business processes". Examples of communication and collaboration technologies include voice, video, conferencing, instant messaging (IM), presence, messaging, calendaring and scheduling while business applications include Customer Relationship Management (CRM) and Enterprise Resource Planning (ERP) solutions.

Nigel Sinclair: http://www.unifiedcommunications.co.za/

FUTURETEXT

IP convergence on the Enterprise: Video, voice, data, images – over a single IP network

- Why? Vendors – FMC
- Enterprise – Single network to manage voice and data.
- However, **no compelling proposition** (no immediate need)
- Potential cost savings (balanced against immediate investment - which companies have reservations)
- A wider approach related to services may work
- Cisco and Communigate Pro (South Africa)

Cisco - Web 2.0 approach; Communigate Pro - hospitals
No commercial relationships as of now
Services led approach

5 Five Across

Five Across, builds social networks for companies to connect with their customers or fans.

Features : Individual profiles, chat, video and photo uploading, RSS and more

Cisco -
Sees growth and boost for revenues
Social networking and the wider Web 2.0 phenomenon as ways to drive Internet traffic over its routers

Goal appears to be to sell the platform itself to consumer electronics companies or large media companies

Cisco Digital Signage

FUTURETEXT

A solution for management, publishing and playback of digital media on networked digital signage displays…to redefine how organizations connect with their employees and customers.

Retailers, banks, governments, hotels etc

More than web conferencing: Also includes Media Tone Network (MTN), for secure delivery of on-demand applications.

WebOffice, which runs on MTN and provides document sharing, calendars, databases and Web meetings.

Targeting small businesses, project teams and departments

Lessons learnt?

FUTURETEXT

- Future is bright …
- Video could be an important driver
- Services and Integration are the key
- Vendors like Cisco will create the effect of moving the market in a certain direction
- New applications not yet common - especially spanning the Enterprise boundary
- Becomes a profit centre and not a cost centre and central to the Enterprise

The SIM implementation: SCWS

- The role of SIM in a Web 2.0 and Mobile Web 2.0 world
- What problems can the SIM uniquely solve?
- Why now? especially with new developments like SCWS.

The main assets of the SIM:

- **Universality:** there's a SIM in (almost) 3 billion mobile phones in the world
- **Portability:** end-users can store their digital life in their SIM as they know that they can transfer it when they switch to a new handset
- **Security:** Main drawback of the Web (lack of federated identity, lack of strong authentication, phishing threat, ...),

To be more specific:

Universality: Standardised : SCWS technology is a standardised environment to deploy applications of operators and their partners

Fragmentation: SCWS could solve the problem of fragmentation of mobile application environments (iPhone, Android etc etc)

Handset customization: Only very big operators can afford handset customization programs, at a very high cost for them, and it still doesn't allow to reach handsets that are bought out of their distribution channel)

Certification: It solves the problem of certification of handset applications as the SIM is a natively trusted environment (applications are deployed under operator control)

Interface now competes with Web based interface like Ajax, Flashlite etc –

Device access: SCWS technology will further evolve and we will get a standardised access to device functionalities especially for the browser which it lacks currently.

Portability:

Port personal data : Subscribers want to port their personal data on their new handsets

Port music : - ex music, pictures, videos, but also their phonebook

Phone book as social network

Social applications based on enhanced phone book – for ex – I am watching a video on a video-sharing site, I can easily forward it to somebody stored in my SIM phonebook)

Social graph: I can also synchronise my SIM phonebook with my social graph on the Web for instance update facebook, twitter etc

Security:

Thanks to the SIM, operators have a role to play in the "**federated identity**" space (as identity provider)

SIM can **add a strong authentication scheme to "federation of identities"** technologies: OpenId, CardSpace, LibertyAlliance (mandatory for "added value" transactions such as mobile payment, mobile banking, government transactions, ...)

SIM can also **"host" applications and security keys of third-parties s**uch as banks, transport authorities, ... (especially for Mobile NFC): see GlobalPlatform technology for "multi-applicative SIM". In this environment, we need a "Trusted Service Manager" at the heart of the eco-system

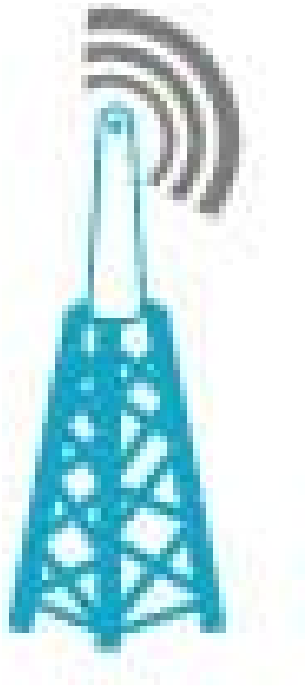
SIM can complement other developments **like two factor authentication for OpenId 2.0**, authentication for NFC etc

Open and closed will both co-exist!
I see a range of options. An unlocked phone(sold with supporting 'coverplans') on one hand – to a completely locked down phone(with remote monitoring and support) and a range of options in between.

This is not speculative. There is some analyst research to back it up.

"Disruptive Analysis expects the handset market to continue to feature both 'operator-locked' and fully-open devices. For example, by 2012, there will be about 250m smartphones capable of supporting non-operator competitive VoIPo3G, plus another 50m mobile broadband enabled laptops. Conversely, there will be over 600m 3G phones in use which mobile operators have restricted or 'closed' in some fashion."

Identity and security implementation ..



Identity enabled IMS Network Services

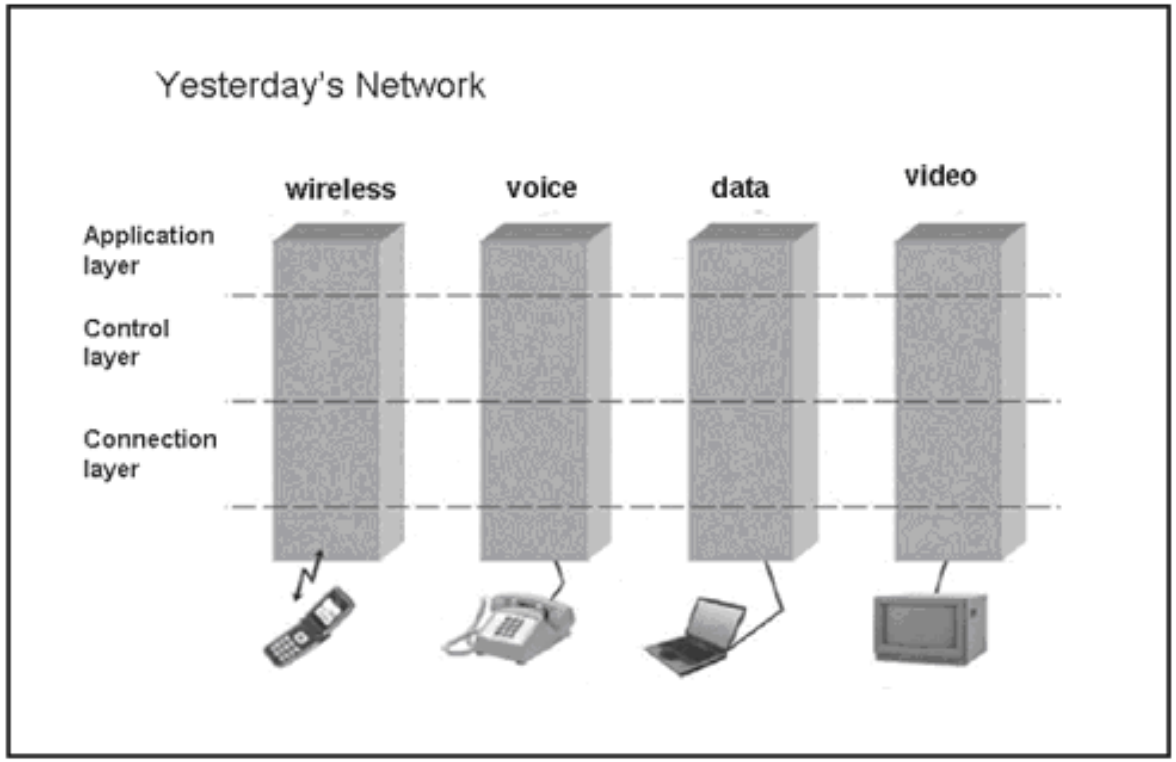


Figure 5:1 Yesterday's Fragmented Network

This section: Identity and Security - by Rakesh Radhakrishnan

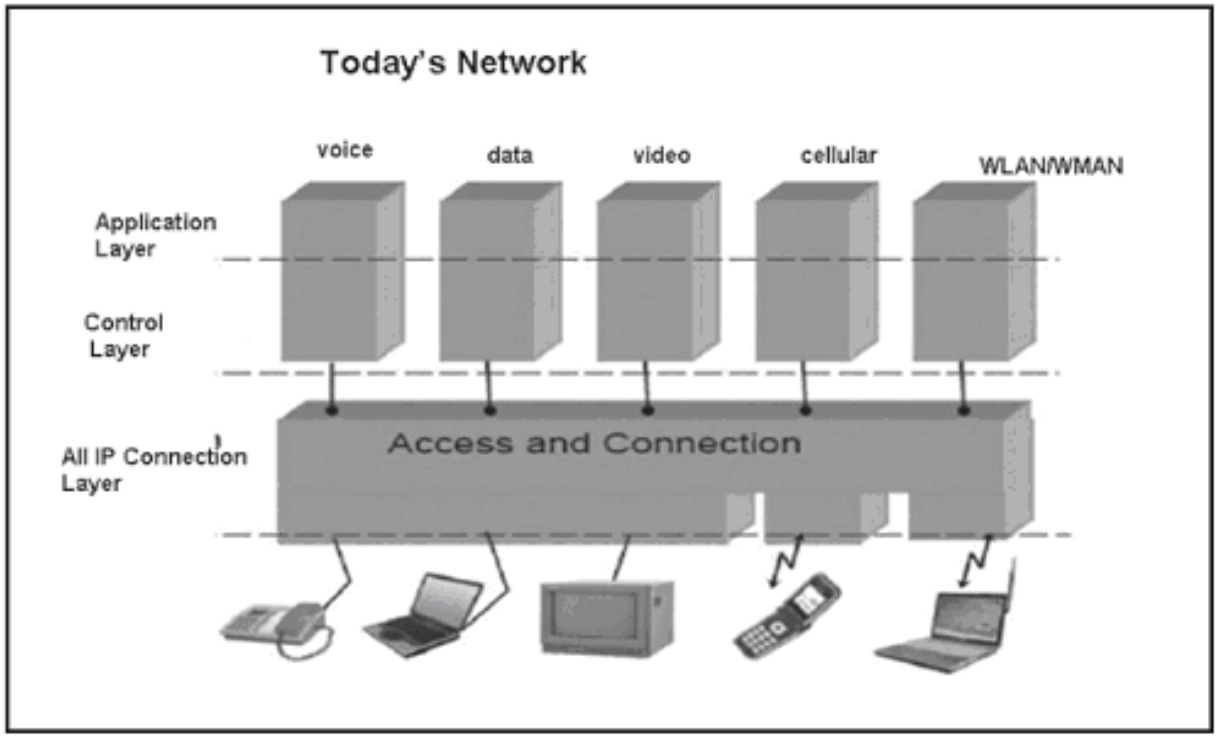


Figure 5:2 Today's Network with a Common IP based Connection Layer

- Evolution of the Telecoms network
- An identity management ecosystem – OpenId, Liberty alliance
- IMS
- HSS
- How they fit together

Identity as a telecoms service (also other APIs), SIP to manage sessions, HSS to hold profile information and all tied to phone which in turn ties back to a federated identity system (Liberty alliance, OpenId)

Identity and Security

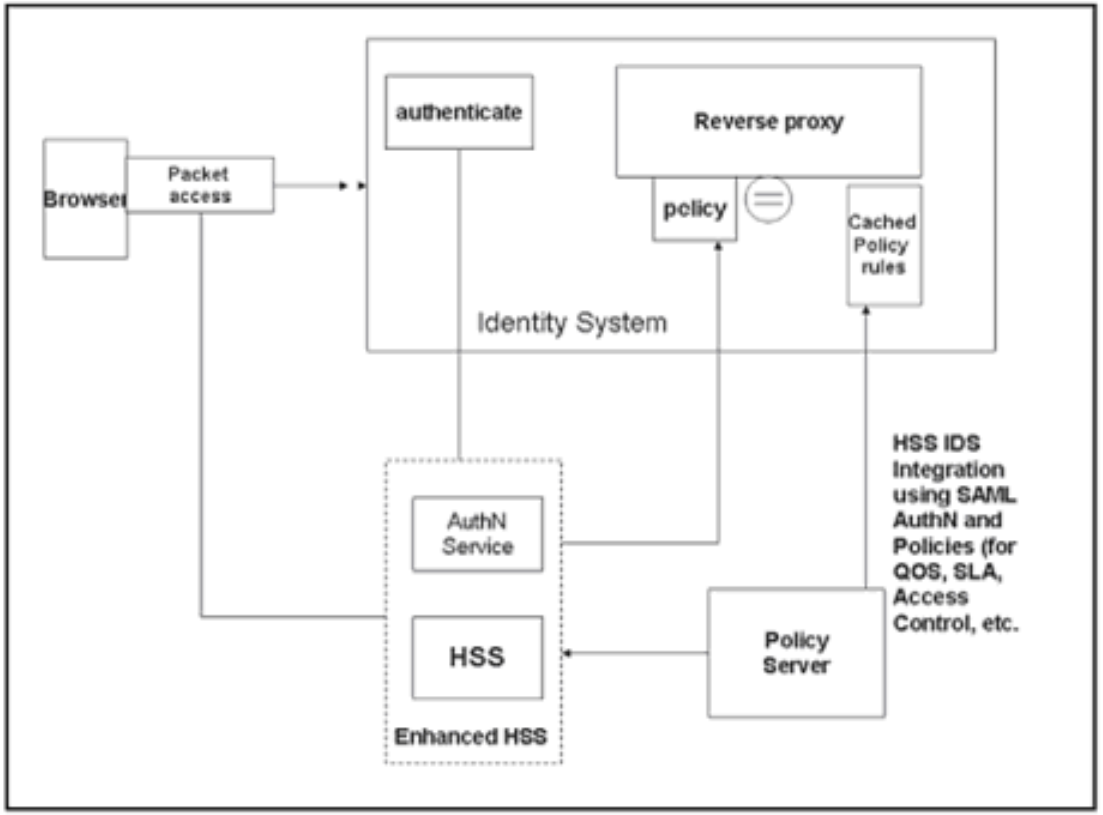


Figure 5:7 Correlated Authentication (Network facing to Service facing)

- **Basic technical validity of the client (requestor):** This includes checks for patches, security fixes, updates, worms, viruses, thefts, and attacks (like spyware and phishing) on the client device

- **Rigid Authentication:** bio-metrics, certificates

- **Establish an Authenticated Session:** wherein the authentication and level of authentication are only relevant and valid for a given Session and there are restrictions applied within the session as well. This is typically accomplished by Access Management solutions, which handle the full life cycle of a Session.

- **Roles:** What rights does the user have. Should be looked at in context of (roles, rules and resource)
- **Rules:** Who can do what.
- **Resources:** The target of Roles and Rules (what) (DRM)
- **Federation:** sharing beyond the regulatory entity
- **Regulation:** Conformance to government regulation
- **Logging, feedback and intervention**

- IMS is a standardised Next Generation Networking (**NGN) architecture** for telecom operators that want to provide mobile and fixed multimedia services.
- It uses a Voice-over-IP (**VoIP**) implementation based on a 3GPP and a standardised implementation of SIP, and runs over the standard Internet Protocol (IP).
- **Existing phone systems** (both packet-switched and circuit-switched) are supported.

- The **aim of IMS** is not only to provide new services but all the services, current and future, that the internet provides.
- Users will be able to execute all their services when **roaming** as well as from their home networks.
- A **multimedia session** between two IMS users, between an IMS user and a user on the Internet, and between two users on the Internet is possible
- IMS truly **merges the internet with the cellular world**; it uses cellular technologies to provide ubiquitous access and internet technologies, to provide appealing services.

- IMS helps the Network **evolve.**
- User **identity** takes on a much greater role in an IMS environment and the HSS is at the center.
- It's helpful to think of the **HSS** (home subscriber service) as the nexus between the IT and the core network worlds.
- HSS acts as the **central repository for** user-related information such as security information (who am I?), location information (where am I calling from?) and user profile information (what services am I subscribed to?) to name a few.
- **HLR ++ ,** No current equivalent but some functionality of HLR (nowhere to store profile and relate to network)

- The notion of **session**. It's a way to provide call control and manage multimedia sessions over IP networks. Today when you make a phone call, a connection is established and torn down the instant you hang-up or attempt to do something else, like send an SMS or take a picture. There's no ability to combine these services together.
- The IETF-defined **Session Initiation Protocol (SIP)** is the basis of a new session-control layer for 3G core networks (IMS).

Home subscriber server

The Home Subscriber Server (HSS), or User Profile Server Function (UPSF), is a **master user database** that supports the IMS network entities that actually handle calls. It contains the **subscription-related information** (user profiles), performs **authentication and authorization of the user,** and can provide information about the **user's physical location**. It is similar to the GSM Home Location Register (HLR) and Authentication Centre (AUC).(wikipedia)

- Evolution of the Telecoms network
- An identity management ecosystem – OpenId, Liberty alliance
- IMS
- HSS(part of IMS)
- How they fit together

Identity as a telecoms service

SIP to manage sessions

HSS to hold profile information

All tied to phone which ..

In turn ties back to a federated identity system

(Liberty alliance, OpenId)

- Liberty alliance - federated identity management
- OpenId - OpenID is a decentralized single sign-on system. Using OpenID-enabled sites, web users do not need to remember traditional authentication tokens such as username and password. Instead, they only need to be previously registered on a website with an OpenID "identity provider", sometimes called an i-broker. Since OpenID is decentralized, any website can employ OpenID software as a way for users to sign in; OpenID solves the problem without relying on any centralized website to confirm digital identity. (wikipedia)
- http://en.wikipedia.org/wiki/SAML Security Assertion Markup Language (SAML)

- For example, a traveller could be a flight passenger as well as a hotel guest. If the airline and the hotel use a federated identity management system, this means that they have a contracted mutual trust in each other's authentication of the user. The traveller could identify him/herself once as a customer for booking the flight and this identity can be carried over to be used for the reservation of a hotel room.
- Federated identity, or the 'federation' of identity, describes the technologies, standards and use-cases which serve to enable the portability of identity information across otherwise autonomous security domains.
- The ultimate goal of identity federation is to enable users of one domain to securely access data or systems of another domain seamlessly, and without the need for completely redundant user administration. (wikipedia)
- Either user centric or Enterprise centric, High trust, Low trust
- Good for security, Identity, End user experience
- It can involve high-trust, high-security scenarios as well as low-trust, low security scenarios.

Identity and Security

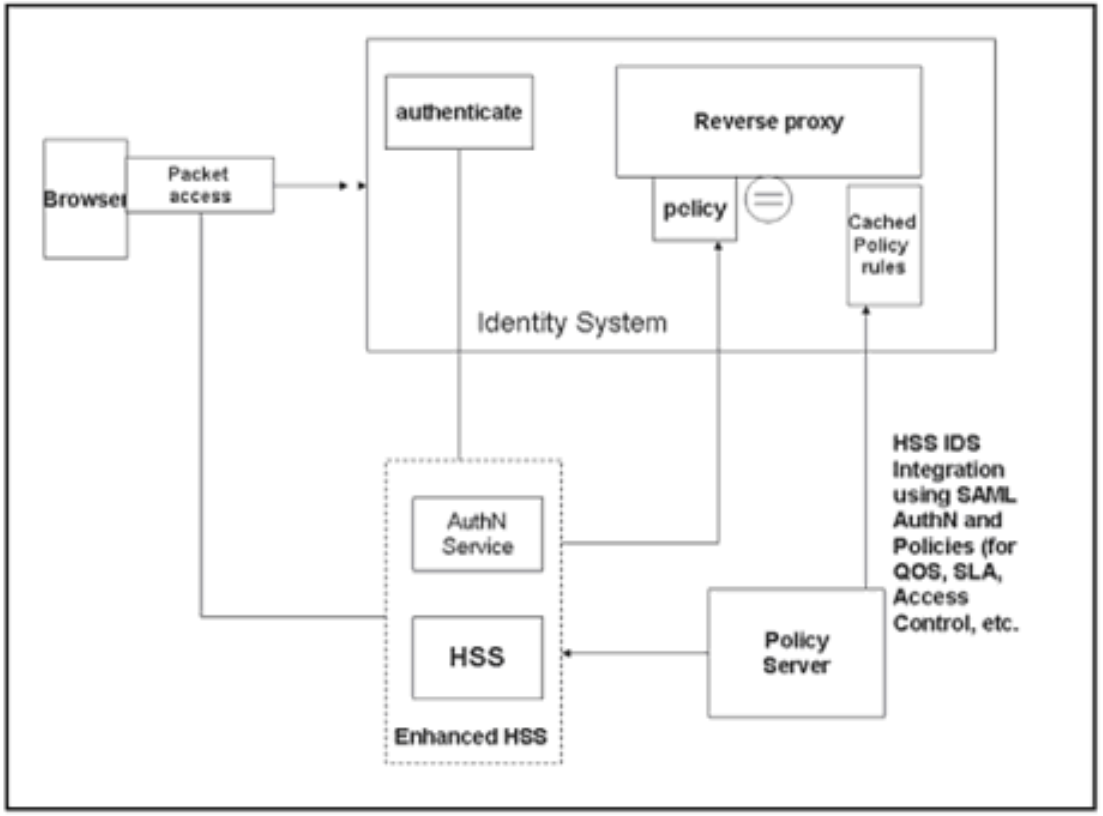


Figure 5:7 Correlated Authentication (Network facing to Service facing)

Identity and SIM

gemalto
security to be free

NFC case study - www.gemalto.com

OpenID - sign-on (i.e., login once using one user name and password for multiple websites/applications) for sites that support OpenID

Alleviates the problem of having to remember multiple user names and passwords

Problems:

a) Problems of single signon – compromised passwords

b) Phlishing - tricks you into thinking your logging in to your OpenID account when you're not.

c) Two-factor authentication provides the solution.

When you provide more than one form of evidence that you are who you say you are.) —something you are (biometrics) and something you have (security token/fob, smart card, etc.).

http://www.mandladventures.com/2008/01/03/more-secure-openid/

New features for users include:

- **Security Improvements** – Heightened authentication procedures dramatically reduce the risk of identity theft and phishing attacks.

- **Attribute Exchange** – Enables OpenIDs to transport detailed profile information including frequent flyer numbers, calendar information and favourite books and movies.

- **Directed Identity** – Individuals who wish to maintain more than one profile now have access to single sign-on without using the same OpenID on each site. (For instance, if AOL sets things up correctly, you'd be able to type "aol.com" into any OpenID 2.0 enabled site to log in with an AIM screen name.)

What is NFC?

Near Field Communication (NFC) is a short-range wireless technology that enables communication between devices over a distance of less than 10 cm. The NFC standard is defined in ISO/IEC 18092.

NFC operates at 13.56 MHz and supports the existing ISO/IEC standards 14443 (Types A/B) and 15693 (tags). An NFC device can work in two modes: active (battery powered) and passive (radio energy powered).

There are three main modes to use NFC:

Card emulation mode: the NFC device behaves exactly like a contactless card and can be used in transport fare payment systems based on MiFare, ISO 14443, Calypso or FeliCa as well as open banking payment systems based on Visa payWave, MasterCard PayPass or American Express ExpressPay.

Reader mode: the NFC device is active and reads a passive RFID tag; for example reading and storing a Web address or coupon from a poster for interactive advertising

Peer-to-peer (P2P) mode: two NFC devices communicate with each other, exchanging

SIM toolkit (STK):

*Smart Card Web Server (SCWS)*3: This powerful technology puts a Web server in the SIM card; advantages are easy deployment of the application (no need to download an application in the handset), consistent rendering across different handset models, and portability when changing handsets

Java midlet (J2ME): A separate, handset-specific application; it is more complex to deploy (requires download) and expensive to maintain (requires specific application for each handset model); advantage is best option for rich graphics

Lifecycle management services include

- Managing the secure remote download of personalized mobile NFC applications
- Managing changes to services over the lifetime of the customer relationship (termination, new handsets, etc.)
- Providing account security and recovery for lost or stolen handsets
- Ensuring security, so mobile operators do not know anything about the service providers' applications, individual accounts or transaction, or managing keys
- Ensuring the support of multiple MNOs – a critical requirement of service providers
- In addition, each application will have critical application-specific requirements the TSM must perform. Mobile contactless payments, s mobile ticketing for transport operators

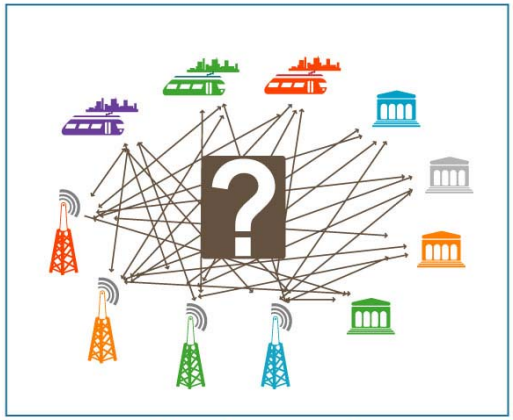
Accelerating Deployment: The Trusted Service Manager

A Trusted Service Manager (TSM)

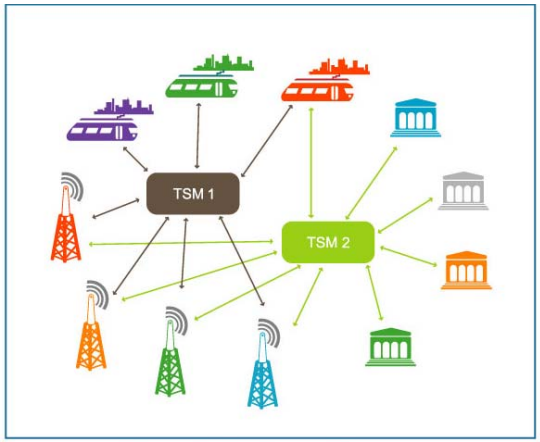
Intermediary

The main role envisaged for the TSM is to help service providers securely distribute and manage contactless services for their customers using the networks of mobile operators.

Option is one to one relationships



The one-to-one approach



Role of Trusted Service Manager

What is Global Platform?

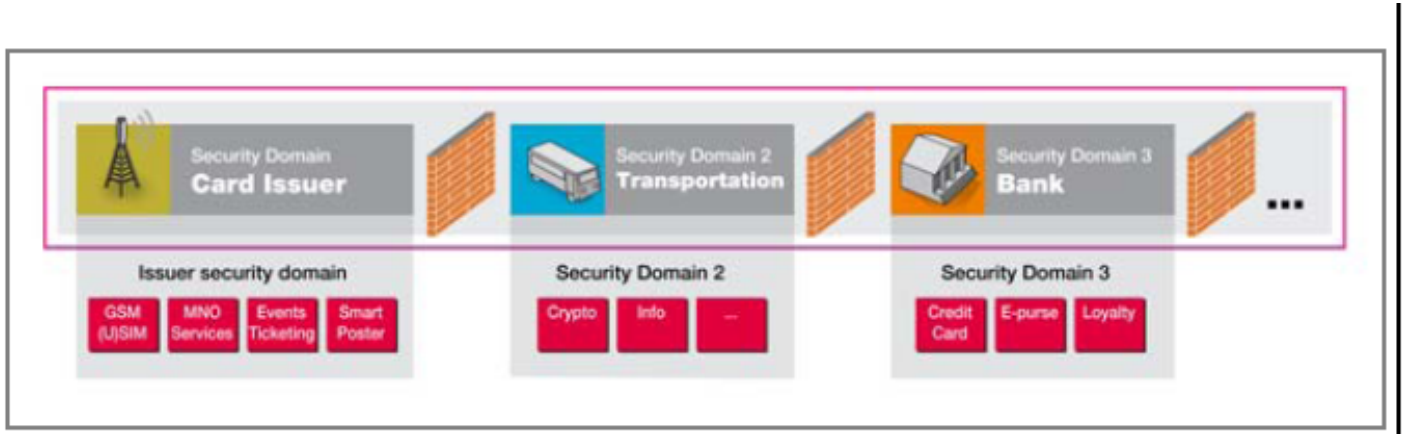
The Global Platform standard is an initiative of JCB, MasterCard, Visa.

It offers a standard and trustworthy framework for putting many different applications on any smart card-based personal device, including bankcards and NFC-enabled SIM cards in mobile handsets.

Global Platform defines a way to guarantee the isolation and security of each application. This means the transport operator can control m-ticketing and the bank its payment application, while the mobile operator maintains complete control of its mobile services subscription. It also defines mechanisms for securely adding and removing these applications in the SIM device at any time.

To make it happen, the Global Platform standard divides the SIM card into independent private spaces called security domains. Each service provider has its own security domain and maintains full control over it; no other service provider can access it or “eavesdrop” on its transactions. This architecture is essential in maintaining a clean breakdown of roles and responsibilities among the stakeholders of the value chain in a multiple service provider framework such as is expected for NFC ecosystems.

www.globalplatform.org



Device API implementation(DOM extensions)

Reference: OpenAjax Alliance (www.openajax.org/)

The implication on the JavaScript side of the proposal that security is implemented within the system is that all APIs could be callable by JavaScript logic; however, if a call is made in a scenario where permission is not granted, then the API call will not succeed.

The proposed conceptual framework has a 4-dimensional model at its core:

Agents - An agent is some person (e.g., the user) or some thing (e.g., a Web site) that are participants in the act of attempting to access a particular device APIs and that have an **identity**. For example, suppose the user is running a web browser to access a web-based mapping service (e.g., maps.google.com) and the mapping service would like to determine the user's current geographic location. In this example, the agents are the user (who on a phone might be identified by his cell phone number) and maps.google.com (identified by domain and/or URL). Composite applications, such as mashup, are more complicated - however the same principle applies

Reference: OpenAjax Alliance (www.openajax.org/)

Actions (including calls to APIs) - Actions are things that might happen, some of which might be subject to a security policy. The invocation of a device API (e.g., retrieving the user's current geographic location, invoking the phone dialer, or determining the battery charge level) is an attempt to make an action occur.

Vulnerabilities - These are the set of known security vulnerabilities that might apply to various service requests. For example, allowing API access to the address book represents a privacy vulnerability. Allowing API access to the phone dialer represents a financial vulnerability because unapproved phone dialing might result in telephony charges to the user. Vulnerability might be assigned strength levels, such as distinguishing between a "privacy vulnerability" and a "serious privacy vulnerability".

Reference: OpenAjax Alliance (www.openajax.org/)

Authorization methods - An operation must be authorized before it can occur. There are a variety of ways that authorization can be granted. The simplest is that the system grants universal access to particular operations. For example, perhaps universal access would be granted to access the current date and time. On the other extreme, other operations might require "root" access, where only the operating system itself and/or a system administrator (for desktop computers) can perform a particular operation. The more interesting area is between the two extremes, where authorization might be granted via a user prompt, or by virtue of a particular software program having a digital signature that can be verified by a particular authority, or because the software is known to come from a particular software suppliers that is deemed to be trustworthy.

Reference: OpenAjax Alliance (www.openajax.org/)

Agent identity : Two main identity types appear to be relevant:

The most familiar model, for packaged applications or widgets that are installable, is the Distinguished Name (DN) of the code signing certificate associated with the signature on the package. The formalised security frameworks for many mobile environments, including MIDP/JavaME, bases an agent's rights on this identity. However, a DN identity may also be a relevant agent identity in other situations, such as where a signed script or web page is loaded from a website using the jar: protocol.

The most natural model for remotely websites viewed in a browser is to treat the URI, or part of the URI (e.g., the domain), as the agent's identity. This usage is probably most familiar in the security configuration in IE, where websites are assigned to security zones based on URI (in fact, on the domain part of the URI, together with knowledge as to whether or not that domain has been verified using HTTPS). Given the domain-level "sandboxing" that is applied in the browser security model, the domain part of the URI is the part that can most naturally and reliably be considered to be the agent identity in this case. Again, this URI/domain identity type might also be relevant in other situations, such as where an unsigned installable package is downloaded from a given site.

Reference: OpenAjax Alliance (www.openajax.org/)

In multiple-origin application models, it is pertinent to ask whether or not there are multiple agents, or multiple agent identities in play.

The simplest kind of multiple-origin application is where a web page refers to a third-party script from another domain, and that script executes within the context of the web page. If the script attempts an action (such as a call to a particular device API), it **is necessary to decide whether it is the identity (i.e. domain) of the containing page, or the domain of origin of the script (or both) that is relevant to deciding whether or not to permit the action. The conventional browser security model makes no distinction between the rights or capabilities of scripts from different origins once they have become within scope within a given page, so it is not possible in practice to rely on any identity in this case other than the identity (ie domain) of the containing page.**

Implied security requirements

A security system should include support for multiple systems of identity for agents, including at least Distinguished Name and URI identity types.

A security system should reliably determine the relevant agent and identity for any attempted action, including multiple-origin applications. (Add some comment here about trusted subsystems where there is a reliable way of separating the agent/identities involved in a sequence of events leading to an action.)

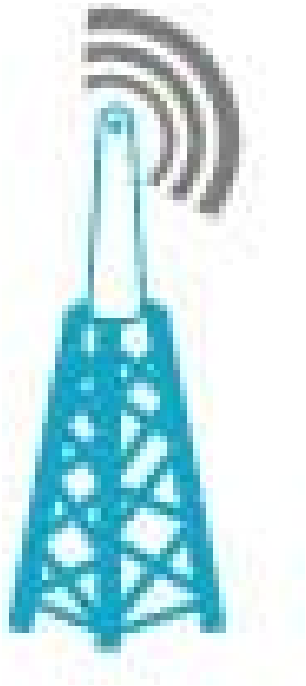
Google Gears

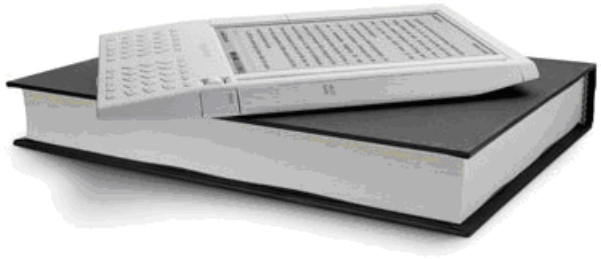
http://code.google.com/apis/gears/security.html

Google Gears uses the same origin policy as its underlying security model. A web page with a particular *scheme, host, and port* can only access resources with the same *scheme, host, and port*.

This means a site using Google Gears: Database: Can only open databases created for that site's origin.LocalServer: Can only capture URLs and use manifests from the site's origin.

Devices with network connections - Kindle





- Amazon pays for Kindle's wireless connectivity
- No subscription
- Devices :Wireless but not a phone
- Probably also the reason for Verizon's opening up!
- Potentially massive market (think of the stock price chart)
-