Mobile Cloud Computing and Regulatory Issues

Have you ever used Mobile Cloud Computing?

Mobile

Processor	**Small**
Storage	**Small**
Network	**Constant Change!**
Power	**Limited Battery**
Sensors/gadgets	**Lots!**
Personal	**Very**

Interdroid: a platform for distributed smartphone applications, H. Bal @el, VU University Amsterdam

Cloud

Processor	**Almost Unlimited**
Storage	**Almost Unlimited**
Network	**Constant**
Power	**Almost Unlimited**
Sensors/gadgets	**None**
Personal	**Not At All**

Interdroid: a platform for distributed smartphone applications, H. Bal @el, VU University Amsterdam

Made for each other?

	Mobile	Cloud
Processor	Small	Almost Unlimited
Storage	Small	Almost Unlimited
Network	Constant Change!	Constant
Power	Limited Battery	Almost Unlimited
Sensors/gadgets	Lots!	None
Personal	Very	Not At All

Pakistan Telecommunication Authority

PTA

A gallery of **disruptive technologies**

Estimated potential economic impact of technologies across sized applications in 2025, $ trillion, annual

	0	1	2	3	4	5	6	7	8	9	10	11

1. Mobile Internet

2. Automation of knowledge work

3. Internet of Things

4. Cloud

5. Advanced robotics

6. Autonomous and near-autonomous vehicles

7. Next-generation genomics

8. Energy storage

9. 3-D printing

10. Advanced materials

11. Advanced oil and gas exploration and recovery

12. Renewable energy
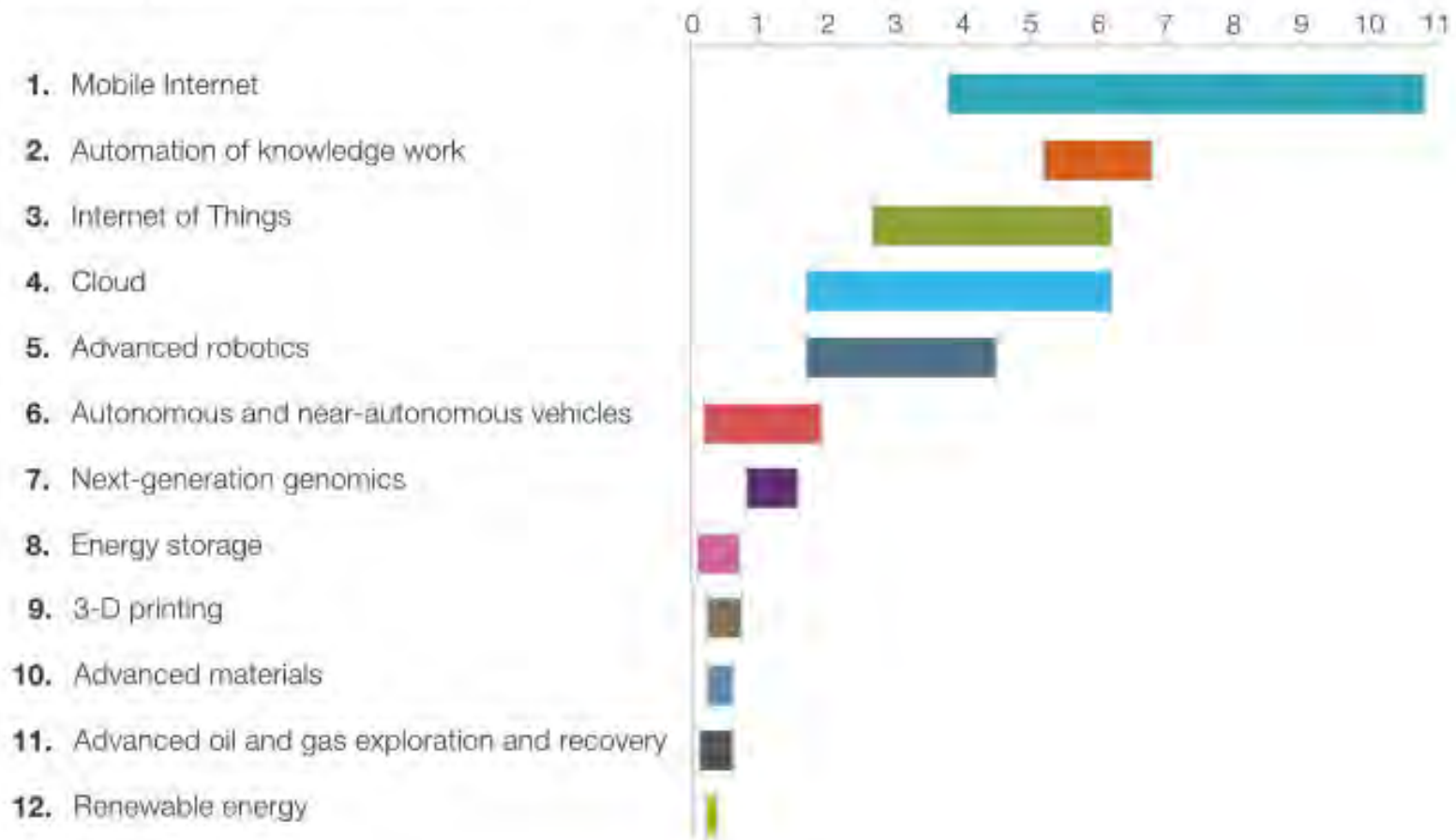
SOURCE: McKinsey Global Institute

Notes on sizing: These economic impact estimates are not comprehensive and include potential direct impact of sized applications only. They do not represent GDP or market size (revenue), but rather economic potential, including consumer surplus. The relative sizes of technology categories shown do not constitute a "ranking," since our sizing is not comprehensive. We do not quantify the split or transfer of surplus among or across companies or consumers, since this would depend on emerging competitive dynamics and business models. Moreover, the estimates are not directly additive, since some applications and/or value drivers are overlapping across technologies. Finally, they are not fully risk- or probability-adjusted.

Mobile Cloud Computing

Mobile Computing is to describe technologies that enable people to access network services **anyplace, anytime, and anywhere.**

Mobile is a significant component of the evolution of computing

Mobile/Wireless/Cloud

Web/Desktop

http://www

Client/Server

Host/Mainframe

Source: IBM

Mobility means changes

Hardware
Lighter, smaller, energy management, user interface

Low bandwidth, high bandwidth variability
Kbit/s to Mbit/s, bandwidth fluctuation

Security risk
Devices more vulnerable, endpoint authentication harder

Heterogeneous network
Different devices, interfaces and protocols

Location awareness
Locality adaptation

Higher loss-rates, higher delays, more jitter
Connection setup time, hand-off/handover

Restrictive regulations of frequencies
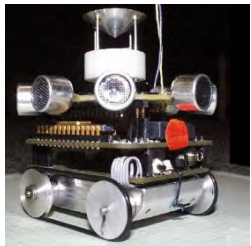Frequencies have to be coordinated
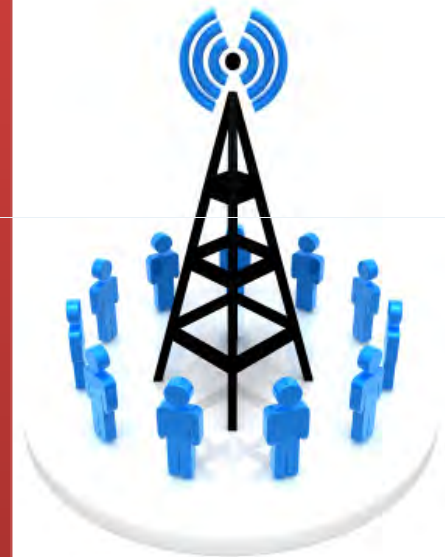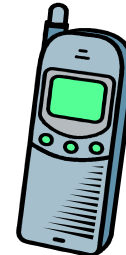
Faster Wireless Connectivity is Required for 2020

Source: http://www.pinterest.com/
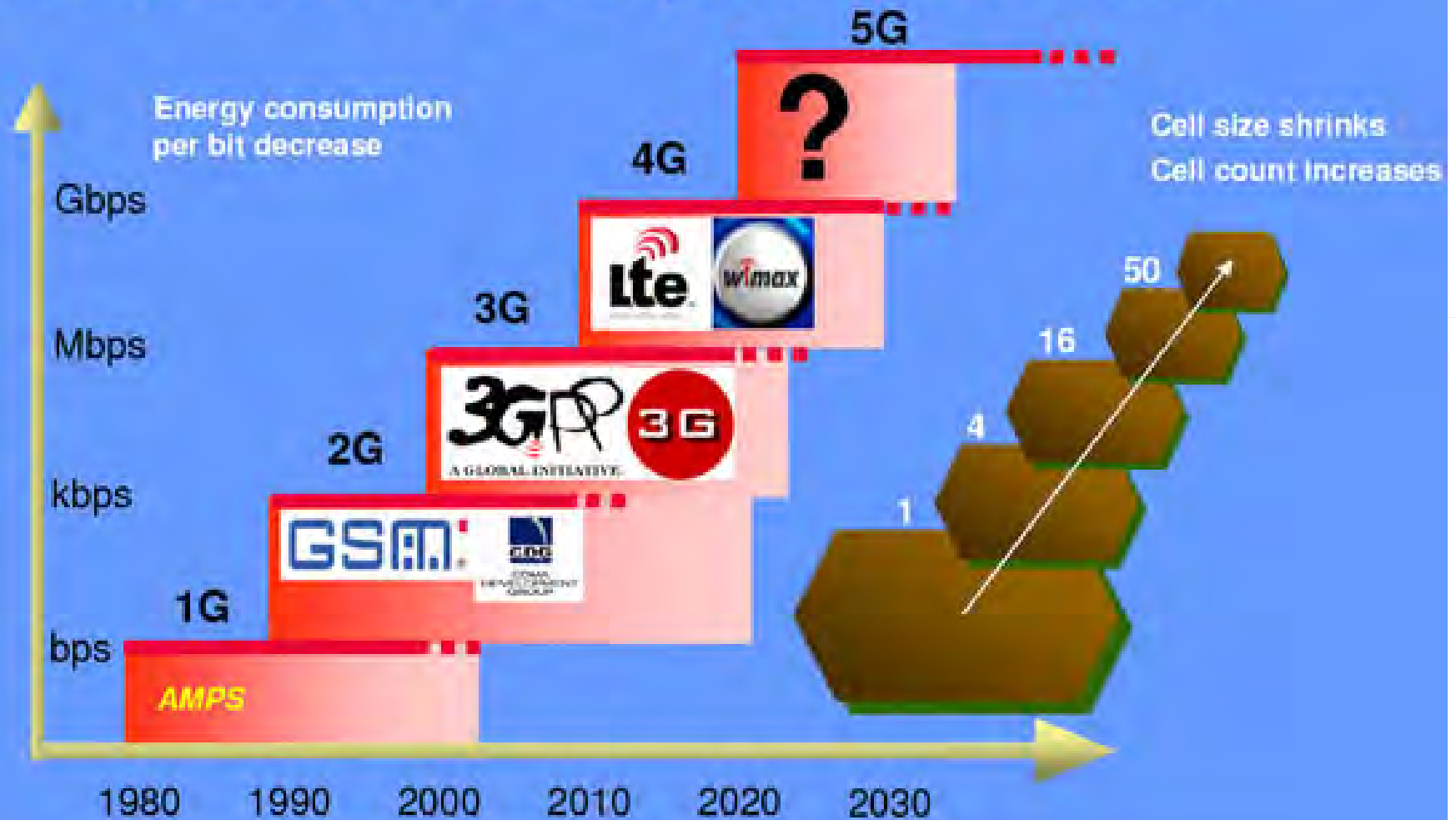
Sensors, embedded controllers
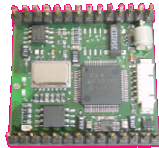
Smart phone
- voice, data
- simple graphical displays

Laptop
- fully functional
- standard applications

Wearable device
- human wearable
- non standard I/O

PDA
- graphical displays
- character recognition

Source: University of Colorado

- **Vehicles**
  - transmission of news, road condition, weather, music via DAB
  - personal communication using GSM
  - position via GPS
  - local ad-hoc network with vehicles close-by to prevent accidents, guidance system, redundancy
  - vehicle data (e.g., from busses, high-speed trains) can be transmitted in advance for maintenance

- **Medical**
  - Nurses/Doctors in Medical offices are now using Wireless Tablet PCs/WLAN to collect and share patient information.

- **Sales**
  - Sales representatives are using Tablet PCs with Smart phones for presentation, transmitting/access information among office, hotel, and customer location.

- **Emergencies**
  - Early transmission of patient data to the hospital, current status & diagnosis
  - Provide mobile infrastructure in dealing with Natural Disaster (earthquake, hurricane, fire, terrorist attacks, war etc)

• Gartner predicts an increased emphasis on serving the needs of the mobile user in diverse contexts and environments, as opposed to focusing on devices alone

• Phones and wearable devices are now part of an expanded computing environment that includes such things as consumer electronics and connected screens in the workplace and public space. "Increasingly, it's the overall environment that will need to adapt to the requirements of the mobile user.

• This will continue to raise significant management challenges for IT organizations as they lose control of user endpoint devices. It will also require increased attention to user experience design."

Source: www.gartner.com

MCC Security Issues

- Protecting user privacy and data/application secrecy from adversaries is key to establish and maintain consumers' trust in the mobile platform, especially in MCC

- MCC security issues have two main categories:
  - Security for mobile users
  - Securing data on clouds

Security for Mobile Users

- Mobile devices are exposed to numerous security threats like malicious codes and their vulnerability

- GPS can cause privacy issues for subscribers

- Security for mobile applications:
  - Installing and running security software are the simplest ways to detect security threats.
  - Mobile devices are resource constrained, protecting them from the threats is more difficult than that for resourceful devices

Privacy Issues in MCC

- Location based services (LBS) faces a privacy issue on mobile users' provide private information such as their current location

- This problem becomes even worse if an adversary knows user's important information

- LBS or any other service using data can also be expensive while roaming

Regulatory Perspectives / Challenges

Consumer Data and Privacy Protection

The expansion of digital technologies has enabled services such as cloud that dramatically changed the way in which services are delivered to and accessed by consumers. Today we face urgency in deciding how to use ICT markets, self-regulation, and regulatory enforcement to protect personal data

Protecting the privacy of consumers' data and ensuring consumers' data is used for the purposes intended are essential safeguards in todays' converged environment

17

Consumer Data and Privacy Protection Contd

Cloud Computing Service providers shall have specific obligations to protect the privacy and confidentiality of consumer data, including ensuring systems and networks are sufficiently secure to prevent unauthorized access. Similarly, enterprise / business data over cloud should not allowed to be exchanged with other companies without the consumer's permission

Regulations are needed to protect consumer's expectation of privacy, protection of personal data; privacy; confidentiality of information and the right to complain for local services delivered / accessed over the Internet

Quality of Service and Experience (QoSE)

Globally, a number of regulators do enforce minimum QoSE requirements to ensure that providers have reliable and uninterrupted services, including access to information in the cloud.

Environmental concerns

Cloud services empower large data centers that consume vast amounts of energy, raising environmental concerns.

Steps may be taken to encourage the cloud service provides to minimize energy use, following International standards for reducing energy consumptions and enabling green cloud technologies

Market Competition

Regulators need to ensure that cloud service providers / ISPs do not engage in conduct that constrains the provision of cloud services for reasons that are not transparent, objective, non-discriminatory and proportionate

Data Security and Standardization

Regulators are required to keep intact regulations that stipulate tight controls on the processing of personal data and its transfer over communication networks. There exist data storage uncertainties over "how and where" in the cloud computing / services world. Therefore, much of the regulation touching cloud computing is associated with data security.

We need to ensure that cloud computing / service occurs in a secure environment (which is a big concern for users), to facilitate the take-up of cloud. Cloud service providers should to comply with "security standards", used widely around the world. There are various cloud-specific standardization initiatives underway, for example, the Cloud Security Alliance (CSA) is working on the Cloud Trust protocol for best practice in the industry. Likewise, ITU's Telecommunication Standardization Sector, Study Group 17 is also working on cloud security.

22

Regulatory Perspectives / Challenges

Set out clear policy guidelines for foreign investors that may be interested in investing in the cloud market

Provide clear investment and operational guidelines

Develop local policy and provide tax rebates as cloud computing saves immense power resources by centralizing and maximizing usage.

Encourage investment in local cloud infrastructure setups – saves valuable forex, creates jobs, develops localized expertise and solutions that are useful to the public and private sector.

Regulatory Perspectives / Challenges

Regulator needs to define the relationship between the cloud operator and the user

Set out data security, confidentiality and service levels expectations

Ensure risk mitigation on part of the operators

Final Words

Should regulators intervene?

Much of the cloud computing market may fall outside traditional telecommunication law, but governments and regulators could facilitate its uptake by removing the perceived barriers.

The major concern remains the security of the Meta data generated by use of cloud services. Equally crucial are questions of privacy, data retention or deletion, standards, due diligence and compliance.

THANK YOU