Regulation and the Internet of Things

15th Global Symposium for Regulators (GSR15)

Prof. Ian Brown

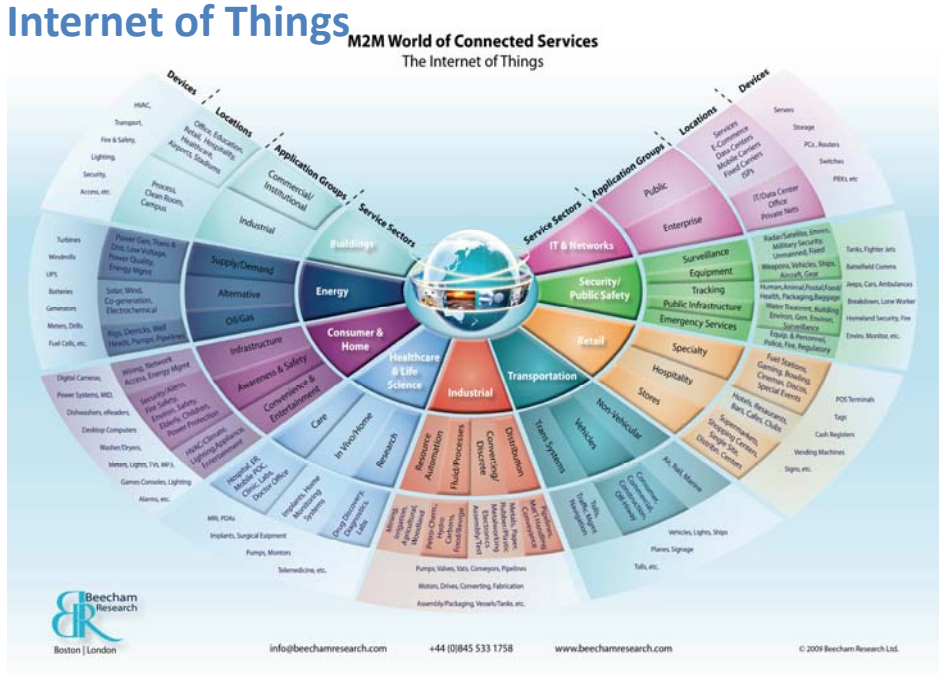
DEFINITIONS

- ITU-T: "A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies."
- Concretely: remotely linked tags, sensors and actuators, increasingly being built into objects throughout the physical world, driven by ongoing rapid falls in the cost of microchips, sensors and communications capacity.
- Protocols: NFC, RFID, medical implants, M2M dedicated networks, ZigBee, Bluetooth, 2G/3G/4G, Wi-Fi, ITS
- Expectations that tens of billions of IoT devices deployed in next decade, driving economic value in $trillions

POPULAR APPLICATIONS

Level	Individual	Community	Society
	 		
IoT	Smartphones Wearables	Connected Cars Health devices Smart homes	Smart Cities Smart Grids
Egs.	GPS, Fitbits Visa PayWave Mastercard Paypass Employee passes	Intelligent Transport Systems Event Data Recorders (EDRs) Blood pressure monitors; remote burglar/heating systems	Smart metering; Smart water meters Traffic monitoring
Data	Mobile money Fitness data, GPS location-based data	Speed, distance, airbag, crash locations/alerts; Heart rate, blood pressure, Diet; remote heating data	Electricity/water consumption & billing; Traffic flow data
Intended Audience	Individual person Immediate friends/ family; banks; employers	GP, health authorities; health & car insurance; Police Wider friends, social networks	Authorities/regulators Utility companies; Other citizens

Internet of Things



REGULATORY ISSUES

- Licensing and spectrum management
- Switching and roaming
- Addressing and numbering
- Competition
- Security and privacy

LICENSING AND SPECTRUM MANAGEMENT

Goal: Ensure spectrum is available for a wide range of IoT applications, at short and long range, in licensed and unlicensed bands.

Best practice: Monitor availability of spectrum for short and long-range IoT communications and backhaul network capacity.

Encourage 4G deployment and use of small-cell technology.

Potential measures: Further experimentation with use of white space and shared-space technology.
Encourage development of LTE-A and 5G networks, and keep need for IoT-specific spectrum under review.

SWITCHING AND ROAMING

Goal: Encourage development of SIMs and mobile network accounts suitable for large M2M users, roaming mobile devices, and fixed devices in areas of poor reception.

Best practice: Mobile network operators develop M2M-specific business units with appropriate billing and management.

Further development and deployment of embedded, remotely provisioned SIMs in M2M systems.

Potential measures: Global agreement on updated E.212 standards, making appropriate use of GSMA standards.

Provision of Mobile Network Codes to IoT service providers.

Source: ITU.

ADDRESSING AND NUMBERING

Goal: Large address space needed for globally addressable things (although many IoT devices only need local connectivity).

Best practice: Deployment of IPv6 by ISPs, public and private sector organisations.

Use of IMSI for M2M applications.

Potential measures: Universal IPv6 adoption by governments in their own services and procurements, and other incentives for private sector adoption.

COMPETITION

Goal: Avoid IoT user lock-in and new barriers to entry.

Best practice: Ensure competition regulators have capability to monitor IoT markets for abuses of dominant positions.

Provide institutional mechanism for ongoing review of laws and regulations for impact on IoT competitiveness.

Potential measures: Consider measures to increase interoperability through competition and consumer law.

Give users a right to easy access to raw data.

Support global standardisation and deployment of remotely provisioned SIMs for greater M2M competition.

SECURITY AND PRIVACY

Goal: Significantly reduce security vulnerabilities in IoT systems let attackers access private data and cause physical harm in cases such as medical devices and connected vehicles.

Encourage security and vulnerability patching of devices.

Smart city vulnerabilities can be hard to fix but present significant safety issues (e.g. in traffic lights).

Ensure individual control of profiles, which can be used to infer sensitive personal information, such as medical disorders.

Reduce potential for discrimination in employment, financial and healthcare services.

Best practice: Ensuring security and privacy from outset of IoT system design process.

Development of co-regulation by all stakeholders to protect security and privacy.

Further development of privacy and consumer protection rules to ensure security testing of IoT systems that process sensitive personal data.

SECURITY AND PRIVACY - POTENTIAL MEASURES

- R&D on more hardware and software security and privacy mechanisms for resource-constrained IoT systems, particularly targeted towards start-ups and individual entrepreneurs that lack resources to easily develop this functionality.
- Incentives for companies to develop new mechanisms to improve transparency of IoT personal data use, and for gaining informed consent from individuals concerned when sensitive data is gathered or inferences drawn.
- Greater use of Privacy Impact Assessments by organisations building and configuring IoT systems.
- Development of further guidance from global privacy regulators on application of the principles of data minimisation and purpose limitation in IoT systems.
- More cooperation between telecoms and other regulators such as privacy/data protection agencies.