Policy and Regulatory Implications of Big Data and Cloud Computing

Paul Ulrich, Senior Policy Manager for Asia Pacific,
GSMA, pulrich@gsma.com

ITU Workshop on Big Data and Cloud Computing,
Tashkent, Uzbekistand, 20 June 2018

Policy & Regulatory Implications of Big Data & the Cloud

1. Big Data
2. Artificial Intelligence (AI)
3. Cloud Computing
4. Regulatory framework for the Internet of Things (IoT);

Evolution in Computing

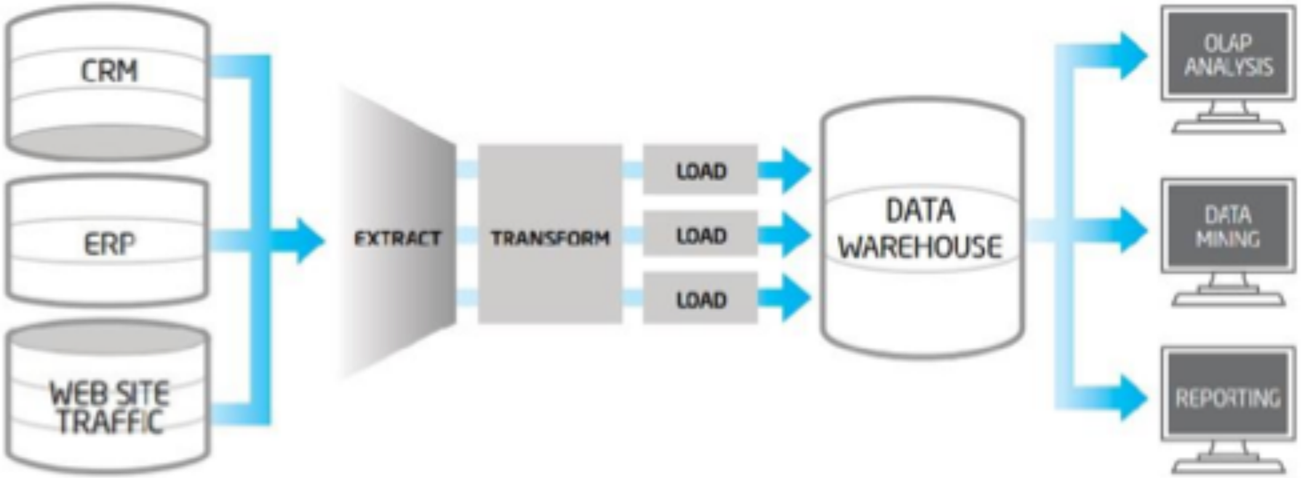
1980s: the Personal Computer

1990s: the Local Area Network

2000s: Data Centers and the Cloud

2010s: (Mobile) Edge Computing

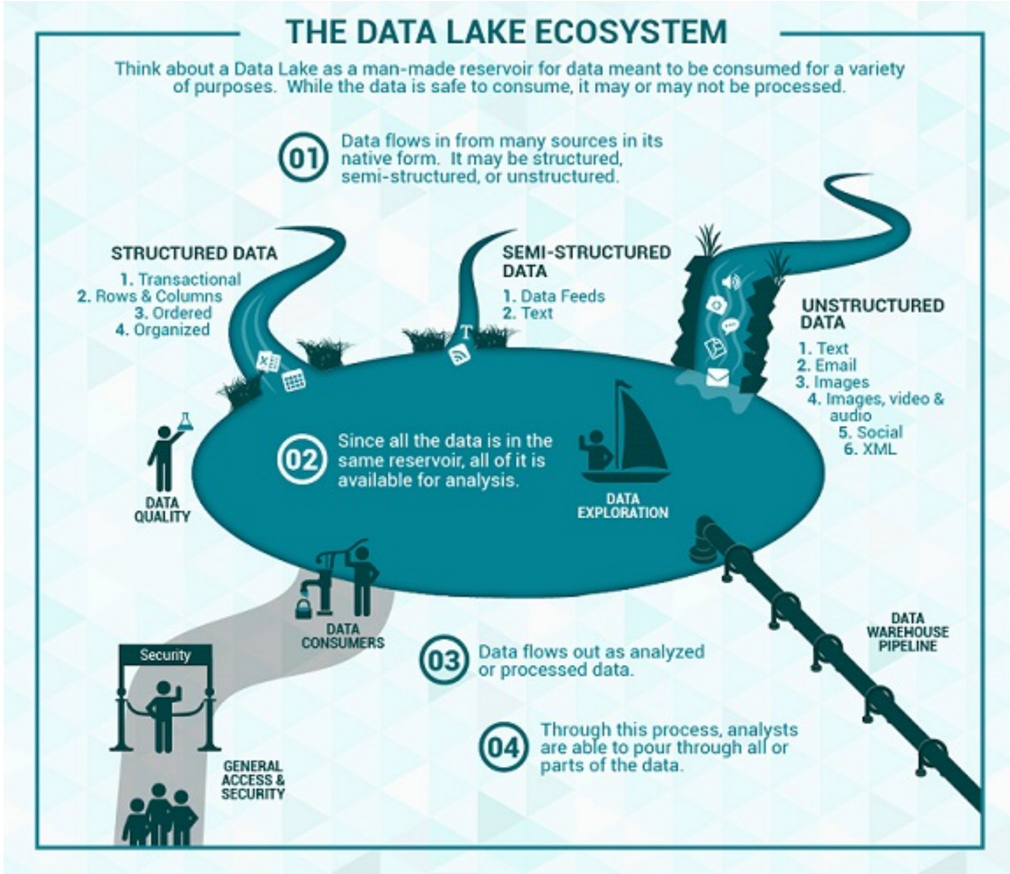
From hard drives to data warehouses for structured data …



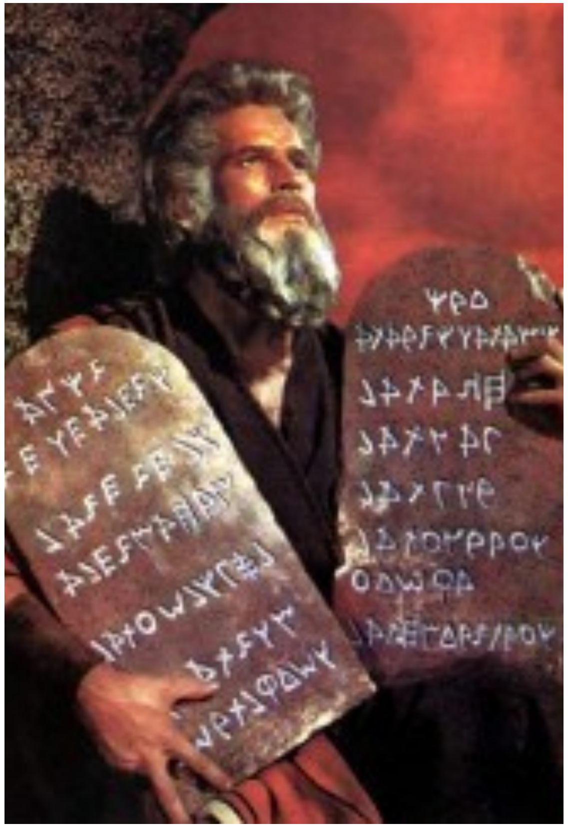
… to data lakes for potentially unstructured data:

1. Organized, partially organised, and unorganised data flow in;

2. Analyzed and processed data flow out – to data warehouses, to data consumers, and for screening by security.

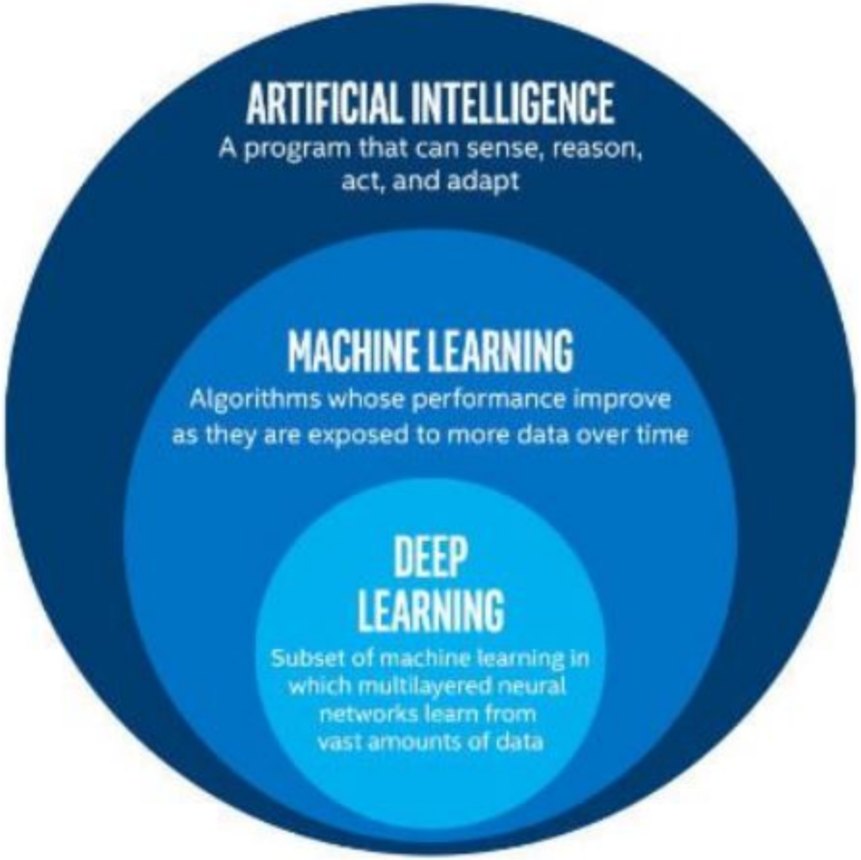


Laws of Accelerating, Exponential Returns on IT



- Moore's Law: speed cost halves every 18 months
- Kryder's Law: memory cost halves every year
- Nielsen's Law: bandwidth cost halves every two years

From AI to Machine Learning to Deep Learning

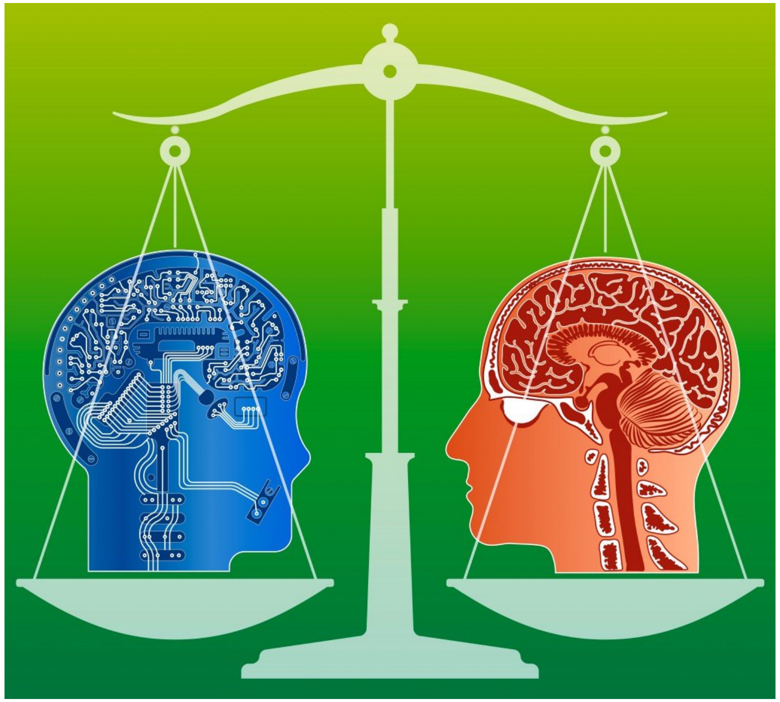


AI: works like human mind, via pattern recognition

Machine Learning: labor-intensive pre-ID'ing of objects with supervised training;

Deep Learning: self-learning, sophisticated algorithms of multi-layered (i.e. "deep") matrix-algebra computations

AI – What can it do?



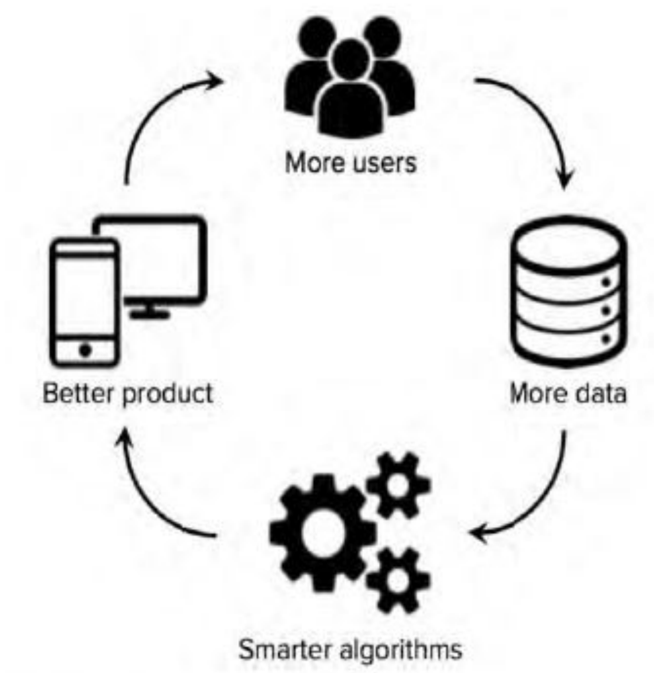
The Singularity is still decades away.

Focus on narrow, rather than general, AI: domain-specific, machine-learning solutions based on specific algorithms for narrow tasks such as customer-service chat bots

AI – machine, man, or both? Results from the chess masters:

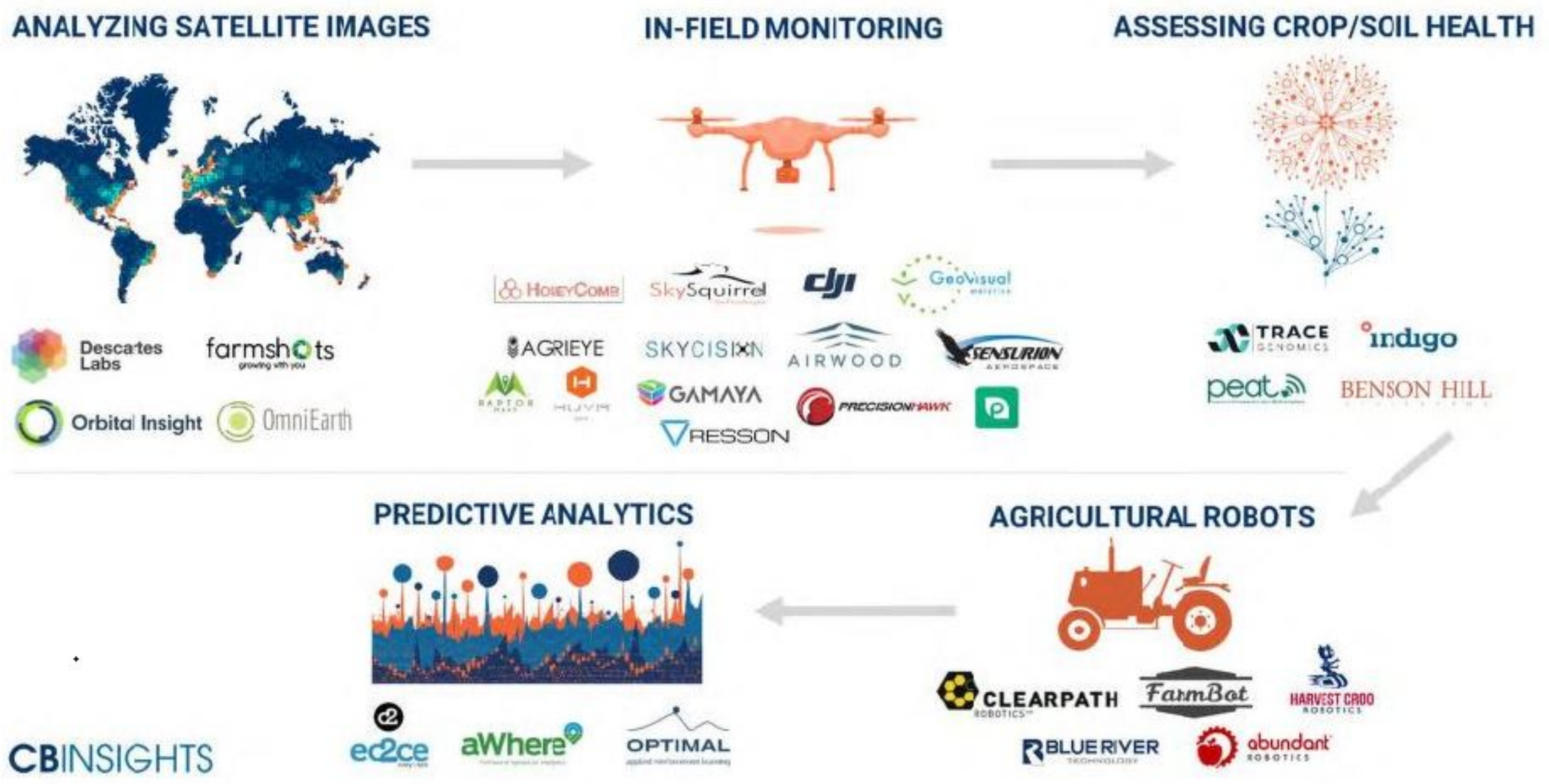
Centaurs or cyborgs, i.e. man and machine in combination, outperform machine alone.

AI – What can it do?



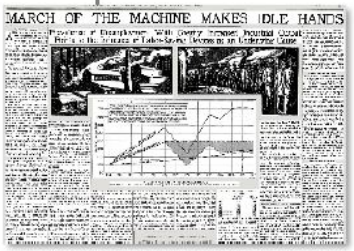
A virtuous circle of more data yielding better algorithms that make for better products and services, which attract more users, who provide still more data …

Sample Uses of Robotics and AI in Agriculture



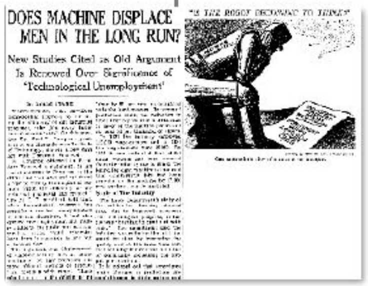
Do governments need to protect jobs from AI?

1920 — 1940 — 1960 — 1980 — 2000 — 2020



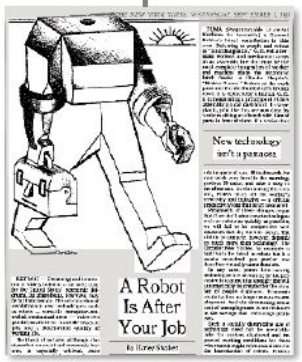
MARCH OF THE MACHINE MAKES IDLE HANDS

200,000 a Year Will Lose Jobs To Automation, U.S. Aides Say



DOES MACHINE DISPLACE MEN IN THE LONG RUN?

New Studies Cited as Old Argument Is Renewed Over Significance of 'Technological Unemployment'



A Robot Is After Your Job

New technology isn't a panacea

Will Robots Take Our Children's Jobs?

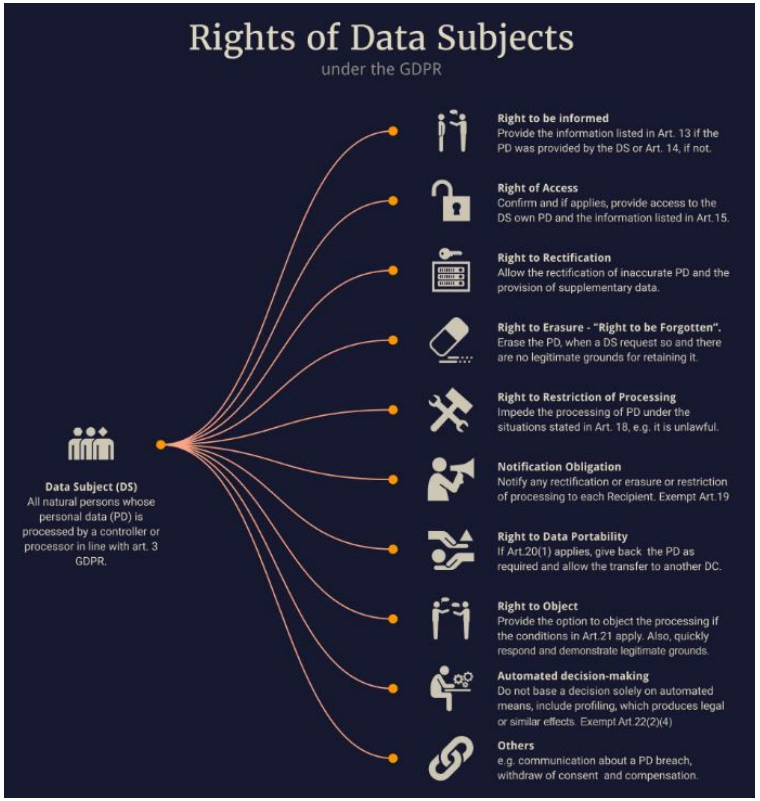
Push for explainable, responsible, ethical AI

Issues of liability for AI

Principles of a Regulatory Framework

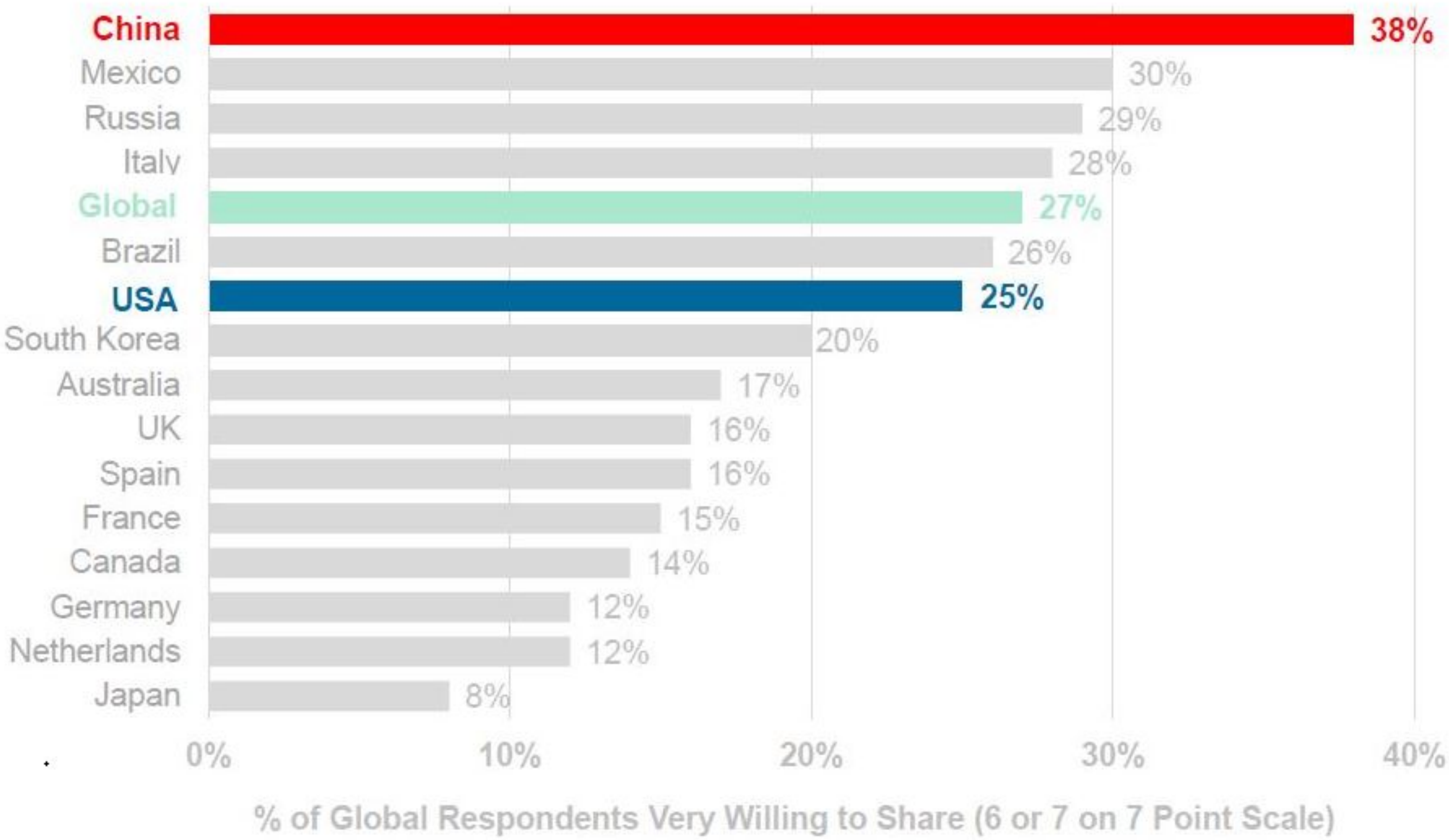
Based on Functionality	Pursue regulatory goals of functional objectives, not legacy structures of industries or technologies
Dynamic	Prefer performance-based approach via *ex-post* enforcement over prescriptive, *ex-ante* rules
Bottom-up Assessment	Consider new approaches to address current realities and whether old rules still apply.

The EU's GDPR versus a possible US approach



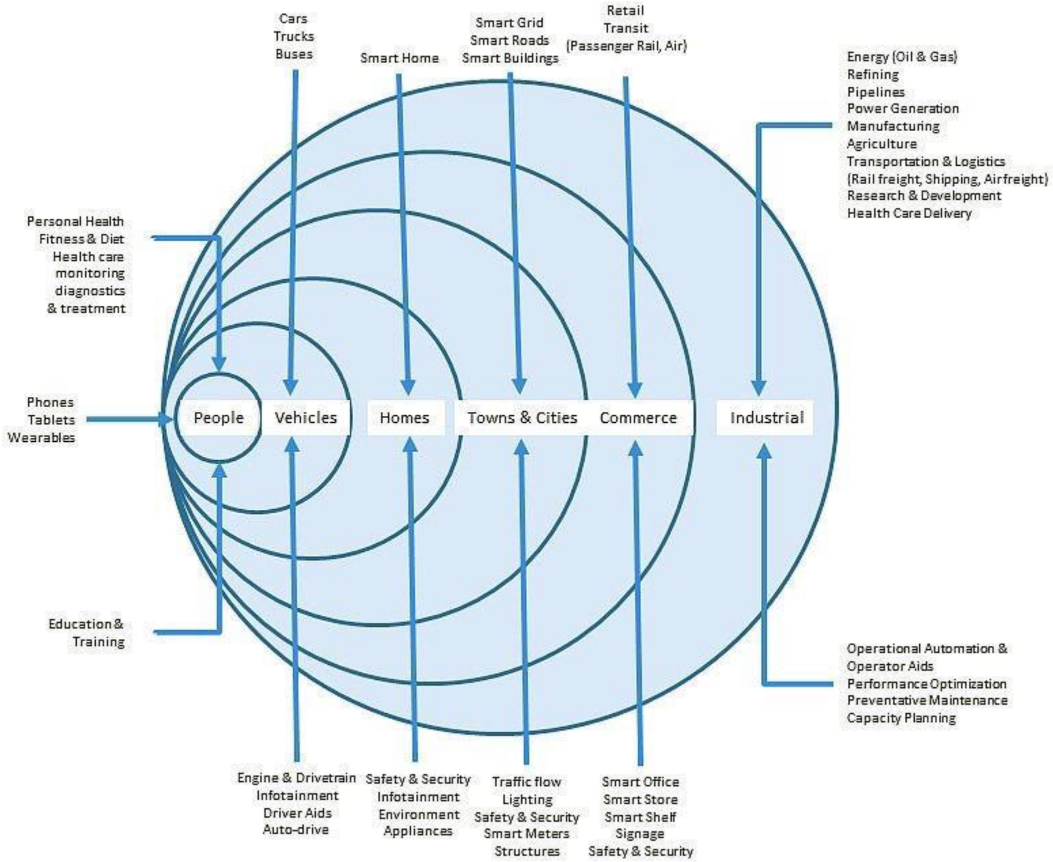
The US Privacy Shield as a workaround for "adequacy"

Willingness to share personal data in return for benefits



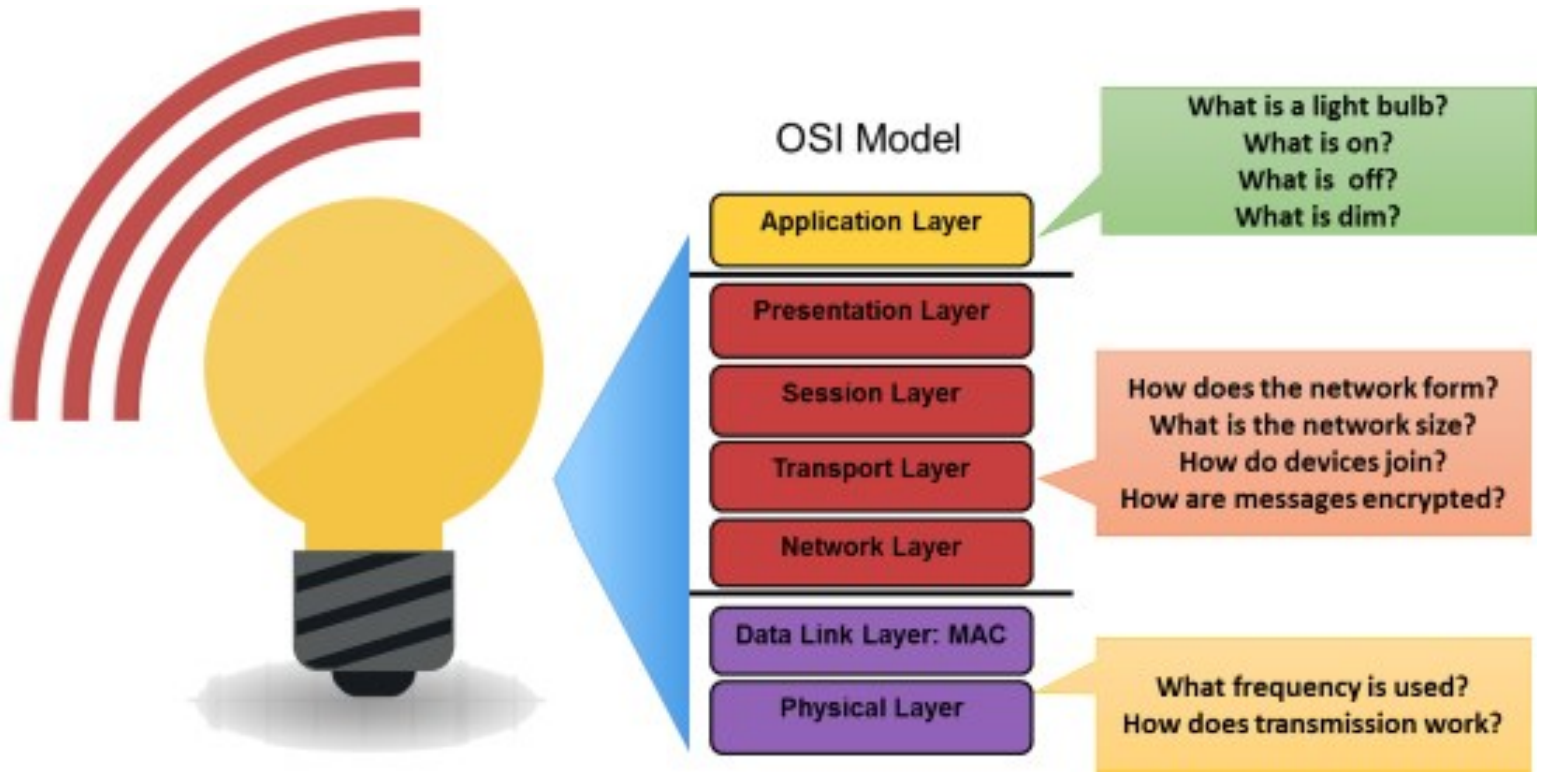
Survey by GfK

The range of IoT-equipped devices: from C-IoT to I-IoT



Source: Based on Goldman Sachs Global Investment Research. Additional analysis by WMG

Technical Architecture for IoT



The IoT will extend across national borders

How will we regulate such IoT data in global supply chains?

Elements of the value chain spread across many countries

e.g. smart cars:

Connected cars made in one country …

… but sold globally with sensors, connectivity, data, and analytics

Data localisation is pervasive …

Policy Rationale	Countries Requiring Localisation
Users' privacy and security	Australia, Brazil, China, EU, France, Germany, Indonesia, Malaysia, Russia, South Korea, Vietnam
Foreign surveillance	Brazil, Canada, China, France, Germany, India, Russia
National Security / Law Enforcement	China, France, Indonesia, India, Russia, South Korea, Vietnam
Economic Development	France, Nigeria
National sovereignty	Indonesia

Source: Chandler and Le, July 2017

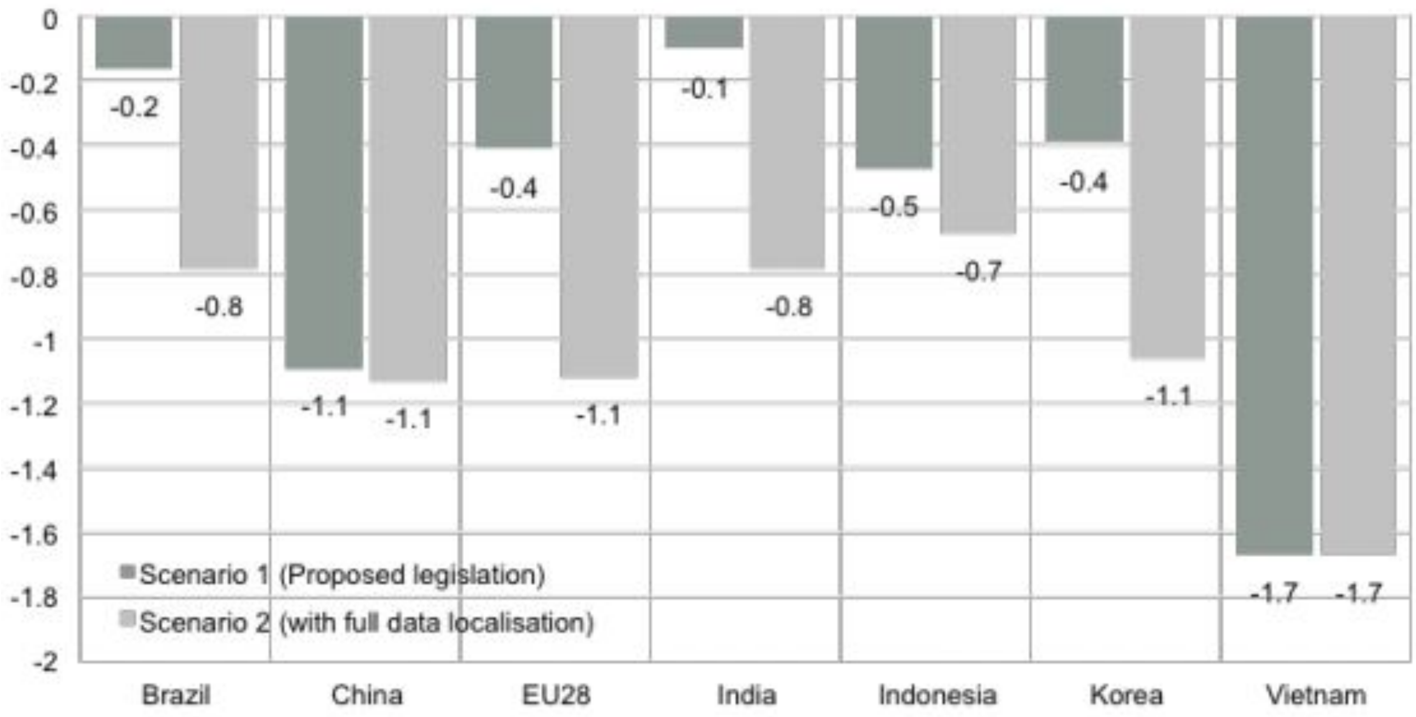
Does data localization increase security?

No. Requiring local storage of personal data:

(i) would not prevent foreign intelligence agencies from accessing it; and

(ii) would weaken users' protection by concentrating data within a single jurisdiction, making it more susceptible to security breaches and natural disasters than if it were dispersed across many jurisdictions.

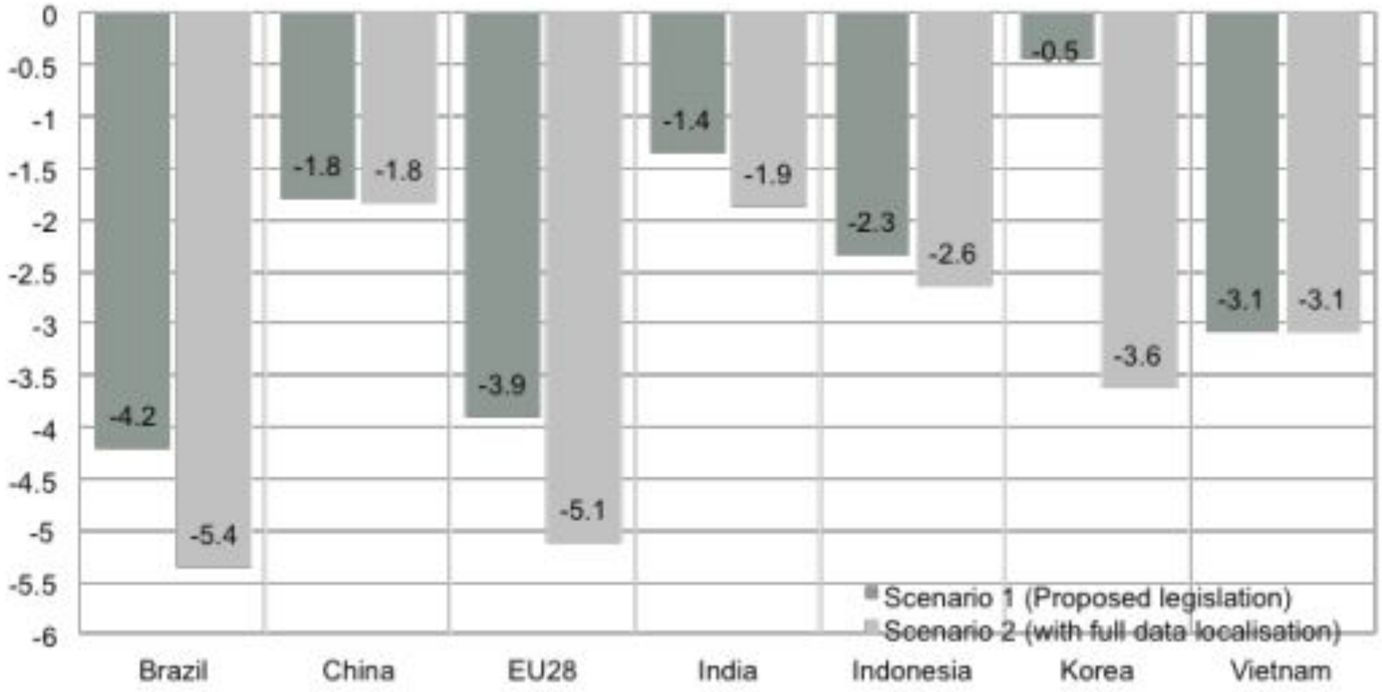
Big Costs from Localising Data (1)



Annual % hit to GDP, by country, from proposed laws and full localisation

Source: ECIPE CGE Simulations, August 2014

Big Costs from Localising Data (2)



Annual % hit to investment, by country, from proposed laws and full localisation

Source: ECIPE CGE Simulations, August 2014

Regulatory framework for the Internet of Things

Three messages from the GSMA for policy makers:

Principle	GSMA's Position	GSMA's Initiatives
1	Support investment and innovation via **interoperable solutions** to reduce deployment costs and facilitate scalability	Mobile IoT initiative in LPWA is an example of industry-led interoperable standards
2	Choose **flexibility** over mandated and specific models of deployment	Remote SIM provisioning shows a flexible solution, tailored to IoT service providers' needs
3	Foster consumer trust in IoT via industry-led **self-regulation** and risk management in privacy and security	The GSMA's privacy toolkit and IoT security guidelines exemplify industry-led solutions to IoT privacy and security.

Regulatory approach to protect IoT

Hackable networked homes, kitchen appliances, door locks, pacemakers, cars – a lot to keep track of

Regulatory approach to maintain IoT

Visual Navigation
Google Maps

Shared Transportation
Mobike

Home Temperature
Nest

Predictive Maintenance
Samsara

Fitness Tracking
Motiv

Precision Cooking
Joule

Who maintains the code if vendor discontinues support or goes bust?

- Make interoperable
- Requirement of a performance bond

New security challenges require new best practices

Companies need to ensure …

AVAILABILITY	IDENTITY	PRIVACY	INTEGRITY
Ensuring constant connectivity between Endpoints and their respective services	Authenticating Endpoints, services, and the customer or end-user operating the Endpoint	Reducing the potential for harm to individual end-users.	Ensuring that system integrity can be verified, tracked, and monitored.

… in services and devices with these characteristics:

LOW COMPLEXITY

- Low processing capability.
- Small amounts of memory.
- Constrained operating system.

LOW POWER

- No permanent power supply
- Possibly permanent, but limited power supply.

LONG LIFECYCLES

- Requires cryptographic design that lasts a lifetime.
- Manage security vulnerabilities that can't be patched within the endpoint.

PHYSICALLY ACCESSIBLE

- Access to local interfaces inside the IoT endpoint.
- Hardware components and interfaces potential target of attackers.

GSMA's IoT Security Guidelines

Referenced By:

enisa

WORLD ECONOMIC FORUM

ECS

Department for Digital, Culture Media & Sport

gsma.com/iotsecurity

Risks of pervasive sensors & monitoring via IoT and AI

About the GSMA