The Internet of Things during Digital Transformation

IoT Applications Regulatory Landscape under GDPR

12/12/2019
Epaminondas – John Bikakis

SECTION CONTENTS : IoT Applications Regulatory Landscape under GDPR

Introduction : Definition for "Internet of Things" – Preliminary Description of a Complex Ecosystem

1. Section 1 : "Internet of Things" Ecosystem within the Digital Single Market Environment

1.1 Sub – Title 1 : IoT Applications for a Single Market : A chance to unleash Europe's strength to Digital Technologies

1.2 Sub – Title 2 : Advancing IoT through a Holistic Approach for Bridging the Digital Divide : A Big Challenge for the 4th Industrial Revolution

2. Section 2 : "Internet of Things" Concerns under the GDPR: Building a New Regulatory Framework for European Data Economy

2.1 Sub – Title 1 : Security and Privacy Concerns relevant to IoT Applications

2.2 Sub – Title 2 : The Internet of Things Regulatory Framework under the European Data Protection Regulation

3. Section 3 : Conclusions: " Internet of Things" Policy in Europe at the Crossroads

Definition for "Internet of Things" Preliminary Description of a Complex Ecosystem

- **First Definition**: "A standardized way for computers to capture information from the real world and to understand it" (Kevin Aston – Mashachussets Institute of Technology's Auto –ID, for Automatic Identification Center in Boston).

- **EU Definition**: "Internet of Things" (IoT) represents the next step towards digitization where all objects and people can be interconnected through communication networks, in and across private, public and industrial spaces, and report about their status and / or about the status of the surrounding environment.

- **Short Description**: With the IoT any physical (e.g. a thermostat, a bike helmet) and virtual (e.g. a representation of a real object in a computer system) object can be connected to other objects and to the Internet, creating a fabric between things as well as between humans and things. So the IoT can combine the physical and the virtual worlds into a new smart environment.

Definition for "Internet of Things" Preliminary Description of a Complex Ecosystem

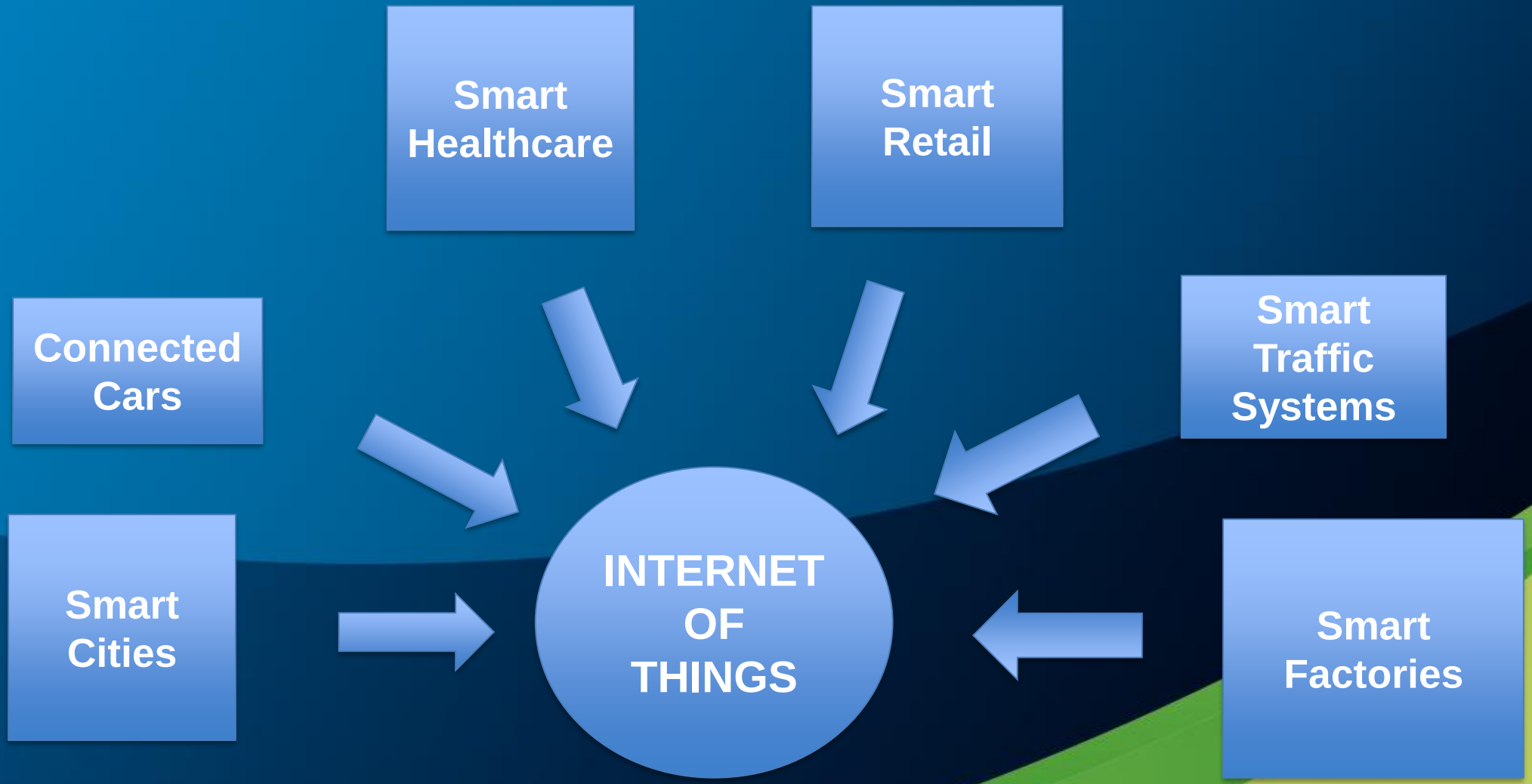
1960s
Birth of the Internet : Internet connects computers between themselves and transmits simple messages with limited data exchange capability

1989 – 2000
A first revolution: Web technologies allow the linking of documents
The birth of **www** (Web 1.0)

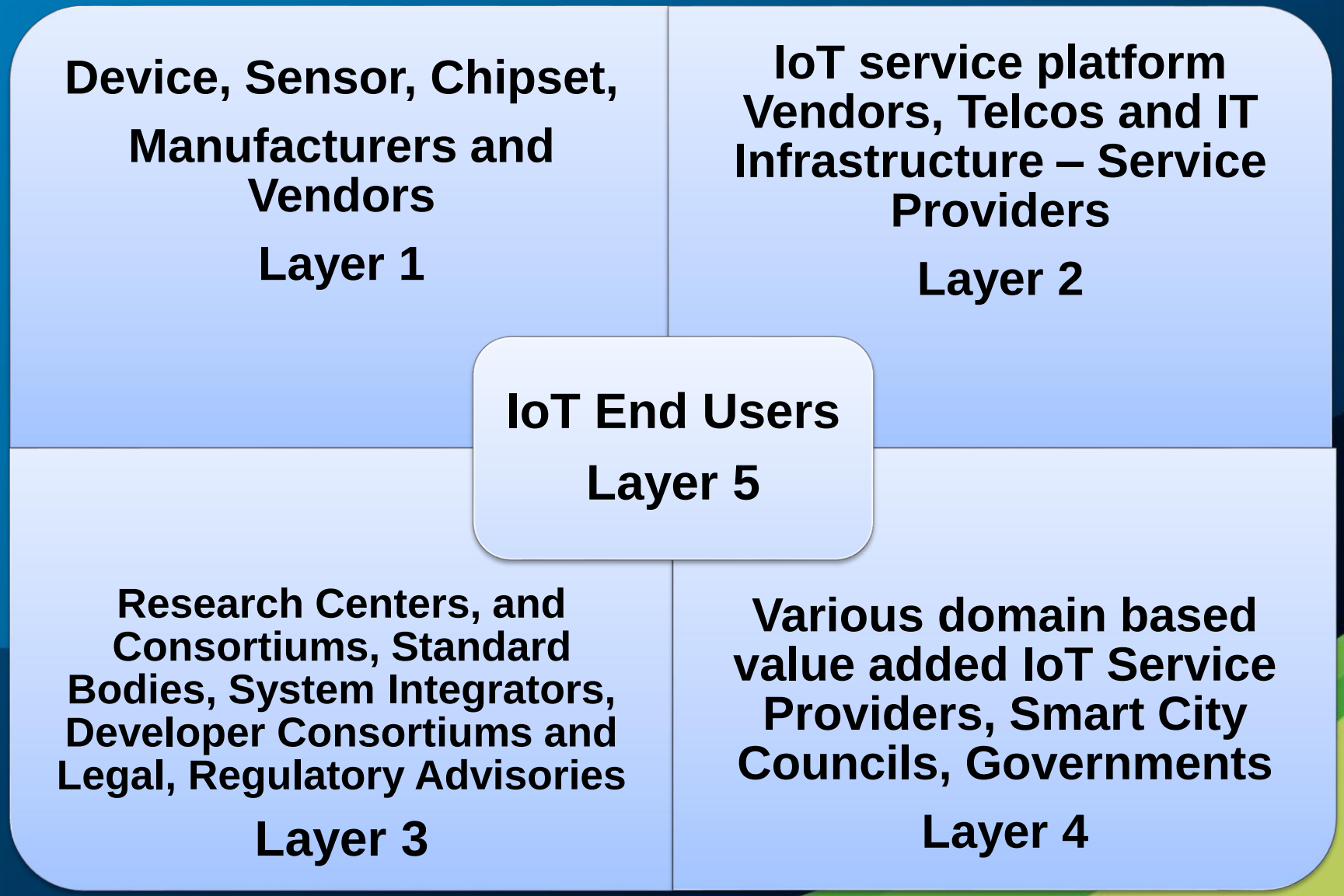
Early 2000s
The Internet becomes Universal: The Internet is now **a universal communication platform.** It carries all **voice, video or information content,** with **social media**, enabling **user –generated content (Web 2.0)**

Now
Internet of Things: "A dynamic global network infrastructure with self – configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities, and use intelligent interfaces, and are seamlessly integrated into the information network" (IERC/ITU official definition)

The “Internet of Things” Complex Ecosystem



IoT End Users (IoT Ecosystem)



“Internet of Things” Ecosystem within the Digital Single Market Environment

Digital Single Market Strategy Main Mission: To maximise the benefits that digital innovation can bring to European Economy, and to allow faster business growth in the digital economy.

- **Digital Single Market (DSM)** technologies and public services modernisation package includes as part of a series of studies and consultations organized by the European Commission:

- The so – called **Digitisation Communication** “Digitising European Industry – Reaping the full benefits of a Digital Single Market”.

- The so – called **Standardisation Communication** “Priorities for ICT Standardisation for the Digital Single Market”.

- **These two communications highlight the importance of Europe becoming a leading region in IoT products and services.**

“Internet of Things” Ecosystem within the Digital Single Market Environment

Within the DSM : To achieve a large uptake of the IoT in Europe **a functioning single market is the point – issue through connectivity, numbering and addressing, telecom networks, data flows and liabilities, as key factors.**

- **A focused standardization effort concerning IT architectures is necessary for mastering all the key elements of the technology and value chain and their integration into horizontal platforms.**
- **A Three – Pillar Approach towards advancement of IoT industry would require action on:**

- **A Single Market for the IoT:** IoT devices and services should be able to connect seamlessly and on plug-and –play basis anywhere in the European Union, and scale up across borders.
- **A Thriving IoT ecosystem:** Open platforms used across vertical silos will help developer communities to innovate. As a kick – start, IoT deployments in selected lead markets will be supported.
- **A Human – Centered IoT:** IoT in Europe is to respect European values, empowering people along with machines and businesses, thanks to high standards **for the protection of personal data and security,** visible notably through a “Trusted IoT” label.

IoT Applications for a Single Market : A chance to unleash Europe's strength to Digital Technologies

- **Europe's Strength in Digital Technologies : Will depend on the capacity of it's industry to seize the opportunities coming from the wider diffusion of digital innovation across sectors.**
- **Development of IoT market offers a unique opportunity for Europe, since it has the potential to lead to the establishment and reinforcement of the new digital value chains in Europe attracting investments and innovators.**
- **Despite the fact that digital transformation of industry is creating tremendous opportunities for Europe, leading industries on IoT Sector have to face huge challenges:**

- Monopolising or ring – fencing of new IoT areas may be an obstacle to the development of these markets, and to the development of open digital platforms.
- Many companies are still cautious when it comes to the IoT and Industry 4.0 implementation as it may involve radical structural changes and radical shift in value creation. This difficulty of adaptation to new business models and new types of alliances, finds its counterpart to the agile players like SMEs, entrepreneurs and start – ups, that be considered to have the potential to seize new opportunities brought up by the IoT.

IoT Applications for a Single Market : A chance to unleash Europe's strength to Digital Technologies

- Lack of common standards and interoperable solutions throughout the products and services life cycles. **Interoperability will be essential for the deployment of the IoT and for ensuring seamless flow of data across sectors and value chains .**
- **The lack of consensus on EU policy coordination in the IoT area, creates five major risks:**

✓ **Risks of fragmentation and a need to address a coordination failure between Member States: National barriers could prevent the IoT from operating on a genuine Single Market basis, which is recognized by the DSM Strategy.**

✓ **Risks of fragmentation between industries: At industrial level a number of areas are already adopting the IoT. However, as in many cases each industrial actor acts unilaterally by adopting separate architectures, standards and business models, something that does not encourage cross – cutting approaches, risks reinforcing silos, and prevention of innovation across areas.**

✓ **Risk of lock – in in proprietary ecosystems, through restraint interoperability and access to data and applications.**

✓ **Risk of users forced to compliance and data sharing instead of developing a human – centered IoT where users can trust the IoT systems around them operate according to understood principles and guarantees for their integrity and security.**

✓ Risk that the uncertainty about business models and standards could generate information asymmetries and market failures, preventing investment and risk – taking.

Advancing IoT through a Holistic Approach for Bridging the Digital Divide : A Big Challenge for the 4th Industrial Revolution

- A Human Centered Character for IoT : Enhancement of trust, security and end - to end personal data protection, and privacy by taking into account the needs of the digital and digitised industry of IoT, constitutes a priority for the European Commission .
- A Cause of Anxiety: Despite the fact that the IoT offers a great potentiality in the everyday living standards, there is a concern may lead to alienation because of objects capable of "talking" to one other and to lose sight of human preferences.
- European Commission Position: A human centered IoT would imply an environment where IoT empower people and not transform them into hostages of technology – The following questions are important for further consideration within this context:

- ❑ How can we ensure end – users fully understand the role, functioning and impact IoT services can have on their lives, choices and environment ?
- ❑ What precautions should we put in place to make sure our medical information can be accessed electronically, but not by the wrong people ?
- ❑ How can all users stay in control of their data ? How can they all, without specific knowledge of underlying technologies, understand the impact of their decisions on what data is shared with whom ?

“Internet of Things” Concerns under the GDPR: Building a New Regulatory Framework for European Data Economy

Liberty requires security without intrusion, security plus privacy (Bruce Schneier)

"Internet of Things" Concerns under the GDPR: Building a New Regulatory Framework for European Data Economy

- **General Statement : IoT enabled smart services are not yet fully secured. Moreover, there are privacy concerns for IoT – enabled service offerings that deal with user data, user – owned device data and data from the environment encapsulating the user or IoT device.**
- **Security and Privacy Concerns : Major roadblocks to the successful deployment of IoT – enabled smart services. "Ensuring security and reliability is one of the three biggest factors holding companies back from realizing the promise of IoT for businesses across all sectors"(TCS Global Trend Study – July 2015 "Internet of Things: The complete reimaginative force" . Retrieved from http://sites.tcs.com/internet-of-things/wp-content/uploads/Internet-of-Things-The-Complete-Reimaginative-Force.pdf)**
- **Big Challenge: The implementation of traditional security techniques for the IoT because of the scale and complexity of IoT - enabled services, presents a unique set of access control challenges due to :**
  - **Low power requirements of IoT devices**
  - **Inability of these devices to run complex encryption algorithms due to memory limitations**
  - **The distributed nature of the extremely large number of IoT devices required to create a system of systems for providing context – aware services.**

Security and Privacy Concerns relevant to IoT Applications

➢ **Basic Categories of IoT Applications to be considered :**

❑ Smart Healthcare Systems :

- ✓ Who has access to the private medical details of patients?
- ✓ Is the data sent from sensors to the gateway device encrypted?
- ✓ Is the data stored at the gateway device?
- ✓ How much personally identifiable information about the patient is being captured and stored?
- ✓ Is the personally identifiable information anonymized?
- ✓ How to verify what information is sent back to the wearable medical device from the remote monitoring center?

❑ Smart Billing and Payment Systems:

- ✓ How is the data from sensors being logged and for what duration? Is the data copied to multiple locations for back – up?
- ✓ Has any personally identifiable information of the customers been compromised ?
- ✓ Is the data safe in transit from sensors to the cloud and from the cloud to the smart phone of the customer?
- ✓ Is the transaction compliant with PCI Payment Acceptance Data Security Standard?

Security and Privacy Concerns relevant to IoT Applications

❑ Smart Home Systems:

- ✓ What data is captured and transmitted by the IoT devices used for this service ?
- ✓ Who can have access the data generated from a home security system?
- ✓ Is the data sent to the actuator encrypted?
- ✓ Is there any authentication of who sends data to the actuator?
- ✓ Does the IoT product vendor have access to the data generated from these devices?

❑ Smart Fitting Rooms and Smart Dressing Areas in Retail Outlets (RFID sensors can be used in smart fitting rooms to allow customers to flip through a catalogue on a touch screen and indicate which items to display in the dressing room):

- ✓ What data is gathered and sent by the sensors?
- ✓ Can the supply chain data be compromised during transit?
- ✓ Does the personal data of customers that are collected by the sensors remain anonymous?
- ✓ Is there any interception of the data gathered by the sensors?

Security and Privacy Concerns relevant to IoT Applications

- **Smart Vending Machines (Customers using smart vending machines select particular products from a display and customer details are tracked immediately from the customer's smart phone by NFC smart – phone payment support fitted to the vending machine for instant e-billing and payment):**
  - ✓ Is the data sent from the sensors to the gateway device encrypted?
  - ✓ Is the customer's financial data exposed during payment?
  - ✓ Can merchants exploit customer information for business benefit?
  - ✓ Is any customer's identifiable information being stored in gateway devices or the cloud?
  - ✓ Is the customer data collected at sensor nodes compromised by any means?

- **IoT Security Concerns:**
  - ✓ Security of IoT Sensors
  - ✓ Security of network connectivity of IoT devices
  - ✓ Security of sensor data and control data
  - ✓ Security of IoT Big Data stored locally or in the cloud
  - ✓ Security for end – to – end control of devices, data, applications and networks

Security and Privacy Concerns relevant to IoT Applications

- **IoT Privacy Concerns:** Privacy is a key concern that needs to be addressed to provide a trustworthy smart service. Globally, regulations on privacy require the collection and processing of personally identifiable information in a verifiable manner. Privacy, therefore, can be broadly classified into the following types:

- ✓ **Identity Privacy:** Data that can disclose a user's or device's identity and as a result should be marked as private.

- ✓ **Location Privacy:** Data that can be used to identify a user's location.

- ✓ **Search Query Privacy:** Search queries can be used to reveal information about the person who made the search query by tracking the IP address of the user.

- ✓ **Digital Footprint Privacy:** IoT – enabled devices, being online all time, can leave behind traceable data about these devices on the Internet. These devices should be secured through effective security protocols to prevent the accumulation of a digital footprint of these devices and the device owners. Also, cookie invasion on IoT devices should be prevented to ensure operational privacy.

Security and Privacy Concerns relevant to IoT Applications

Security

- What is the security architecture of the IoT service?
- How the business functions and data flows are protected through application security, data security, functional control?

Compliance

- Healthcare Services
- Payment Card – Acceptance Data Security Compliance
- Automotive IoT and Connected Cars – Existing and upcoming regulations.

Privacy

- EU GDPR
- Service based Privacy Laws in different countries and regions (existing and upcoming)

Conclusions: “ Internet of Things” Policy in Europe at the Crossroads

Time to trust in the IoT and make a step further to an “Open” European Data Economy

Conclusions: " Internet of Things" Policy in Europe at the Crossroads

- **Security and the protection of Personal Data issues:** Constitute a Key Concern for a successful take up of the IoT.
- **IoT Technology :** Despite the fact that it is found at it's early beginnings, several recent examples of object hacking have shown that - the number of attacks is destined to grow exponentially if known vulnerabilities persist - as connected objects are increasingly used.
- **The crucial issue of Security Authentication:** Networked devices that exchange data with other IoT devices need to be properly authenticated to avoid security problems ; This may need to include certain authentication protocols, moreover to use integrity – secured or encrypted channels of communication.
- **European Commission's Interest:** It considers important to reflect upon possibilities for certification of networked devices that would provide a minimum level of secure authentication from the hardware level to network integrity . This process would entail some analysis of the functions with which each device is equipped, secure data processing and connectivity for the devices to which data are transmitted.

Conclusions: " Internet of Things" Policy in Europe at the Crossroads

…*and to make a step further:* **IoT merges physical and virtual worlds, creating smart environments . It has become a common effort by the European Commission, Member States of the EU, Industry, Organizations and Academic Institutions to unleash the potential of the IoT technology across EU Member States and beyond.**

- **IoT represents the next step towards the digitization of our society and economy, where objects and people are interconnected through communication networks and report about their status and / or the surrounding environment.**

- **So the Question is and will be ?? Is the European Union Area mature enough to make a step further for Building a stronger European Data Economy and remove any data localization restrictions for non – personal data flows in the beginning of the common "European Data Space" ?**
- **…and the answer is definitely : We are in the beginning of a Big Digital Transformation.**

Thank you for Your Attention