Re-imagining Government Through Innovatitve Technology

GOVERNMENT AND THE INTERNET OF THINGS (IOT)

FINDINGS AND RECOMMENDATION OF ATARC'S
INTERNET OF THINGS INNOVATION LAB
NOVEMBER, 2015

IoT Innovation Lab Sponsors

IoT 101 – Defining the Internet’s Next Big Thing.

IoT is changing the way we think about the Internet

Quickly emerging as the “third wave” in the development of the Internet, IoT has the potential to increase the number of devices connected to the Internet by as much as 10X in the next 5 years

An evolving definition of IoT

- Initial definition focused on “things”: “The network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.” – Gartner
- Today we define it more broadly: “An infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react.” – ISO/IEC JTC1 Special Working Group 5

IoT 101 – Everything’s connected

- IoT is a growing network of consumer products and industrial machines – “things,” powered by communication networks and systems and software that allow us to make use of the data.
- IoT is virtually anything you can think of connected to the Internet, from cell phones, kitchen appliances, cars and wearable fitness devices, to jet engines, electricity meters and windmills.

“If it can be connected, it will be connected”

Today there are 2 billion smartphones and 5 billion cell phones in use fueling IoT. By 2020, Gartner estimates there will be 26 billion internet connected devices. Others estimate this number could be 2 or 3 times as high.

Economic Impact:
$11 TRILLION by 2025 according to McKinsey

What does IoT mean for you?

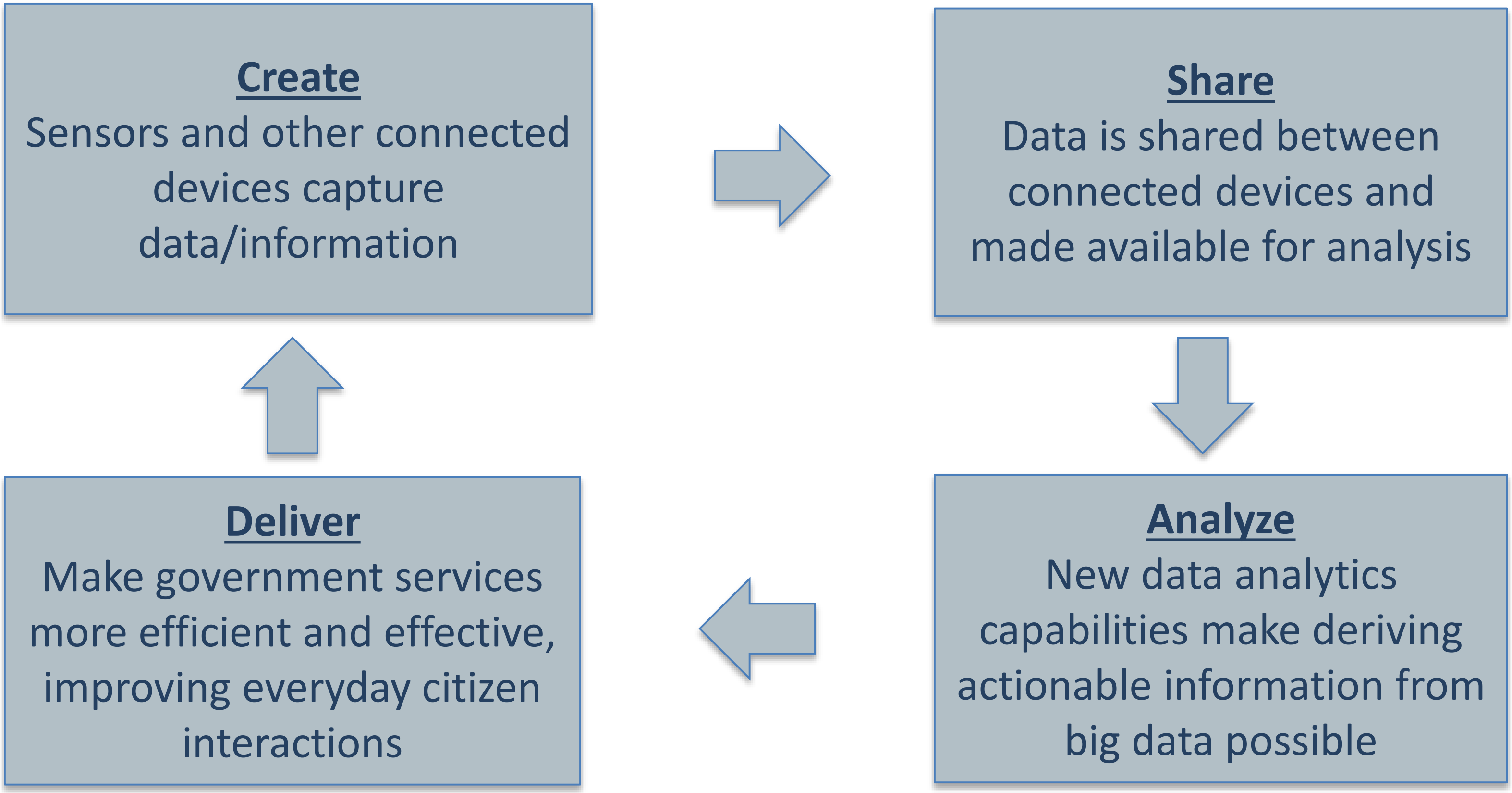
As a citizen – Increased awareness and opportunity in a host of areas, such as healthcare, community services, government services, commerce, marketing, etc. as real time data is collected and made available for use.

As a government employee – New and innovative technologies are being introduced, changing the way we track and interact with citizens. The next stage in building a responsive digital government.

Early adopters – cars, wearables, home appliances, transportation systems

Extracting value from IoT data

The IoT Value Lifecycle



Create
Sensors and other connected devices capture data/information

Share
Data is shared between connected devices and made available for analysis

Analyze
New data analytics capabilities make deriving actionable information from big data possible

Deliver
Make government services more efficient and effective, improving everyday citizen interactions

Technology enablers: What's driving the growth of IoT?

Changes in technology are fueling the rise of IoT. Here's what we see as the drivers:

Apps – The enormous growth of app development is driving personalization and a more citizen centric approach to government and a demand for open data.

Sensors – Today's sensors are smaller, cheaper and more easily deployed. You find them in clothing, on highways, and just about anywhere else. These sensors are driving growth in connected devices.

Smart phones – Smartphones are the hub for IoT. Our phones house apps connecting our homes, cars and health and fitness devices. These connections fuel IoT.

Infrastructure and bandwidth – Critical to the long-term success of IoT is an investment in infrastructure and expanded bandwidth to build out wireless networks that will allow for communication between connected devices.

Technology enablers, continued

Big data – IoT is generating an unprecedented amount of unstructured data, leading to storage and related concerns.

Data analytics – Analytics is the enabler. Big data without analytics will not produce the benefits expected from IoT.

4G and WiFi – WiFi and 4G technologies are ubiquitous today, allowing for nearly universal access and full time generation and collection of data.

IPv6 – The transition to IPv6, and the near limitless number of IP addresses that can be handled by this transition, is a critical step to support the development of IoT as more and more devices are connected.

Software expands the IoT platform

- To fuel IoT growth, standards that allow varied IoT devices to communicate seamlessly with and across common software platforms must be developed.

IDC estimates that 20% of all IoT spending will be on software

- Software translates data into actionable information
- The software that powers IoT will provide a foundation for growth of the IoT platform by managing communications between and among multiple “things.” Think about:
  - App development
  - Identity management
  - Big data processing
  - End-user interface
  - Business process management

What’s government’s role?

Is government a user, a regulator, or somewhere in-between?

- **User -** Makes government more efficient, work better for citizens
- **Regulator –** Standards development, common definitions, promoting interoperability
- **In-between –** Encourage growth, setting a framework for effective application, while balancing competing priorities

The role of the Administration and Congress

IoT is a careful balancing act for policymakers. On one hand they should encourage policies that enhance the growth of IoT. While on the other, they must recognize the need to protect privacy.

What’s government’s goal (as a user)?

Government must figure out its vision for IoT. Once you determine the vision, then you have to figure out if you have the tools and authority to carry the vision out. IoT must serve to improve government operations. Here’s the value proposition:

Enhance the mission	Leverage IoT to improve mission critical functions
Increase productivity	Data and functionality are enhanced via IoT
Reduce cost	New technologies help reduce the cost of government
Reduce consumption	Critical IoT technologies save energy and increase efficiency

What’s government’s goal (as a regulator)?

- IoT raises new and often difficult to answer questions about how to effectively regulate the collection and use of data.
- Despite a lot of talk, there’s no IoT-specific regulation on the horizon
- But as we move forward, here are some things to think about re: regulation:
  - Does one set of regulations work across the entire spectrum of IoT (the answer is likely no)?
  - Regulation should be market driven, encouraging growth, not restricting it
  - Any regulation should be subject to a cost-benefit analysis
  - How do we protect privacy and enhance security?

Developing a National Strategy for IoT?

- Both the US House of Representatives and the US Senate* have passed resolutions calling for a National Strategy to maximize the opportunity of IoT. According to the resolutions the strategy should seek to:
  - Empower consumers and foster economic growth
  - Allows for innovation and prevents misuse
  - Recognizes the importance of consensus based best practices
  - For government: improve efficiency and effective and cut waste, fraud and abuse

*H.Res. 195, S.Res. 110

Challenge Area 1 – Enhancing Cybersecurity

The Internet of Things Needs Its Own Security Model.

Every IoT endpoint and network connection is a potential security risk -- particularly when they're physically accessible to hackers

- **Protecting and securing IoT assets**
  - IoT hardware, Sensors, Data loggers, Routers, LAN/WAN, Cloud and IT Systems
- **Secure transport Wireless (Cellular) and Wireline Networks**
  - 4G, Wi-Fi, BT, RFID and LAN/WAN
- **Effective and secure way to manage identity and data integrity**
  - IoT devices identification, Management, Trusted apps, and SW updates
- **Protect critical infrastructure tampering**
  - Power grids, Manufacturing plants, Utilities, DOD and Finance
- **Ensuring privacy and regulatory compliance**
  - Unauthorized access, HIPAA and PCI

Challenge Area 2 – Protecting Privacy

Addressing privacy issues is paramount to encouraging the growth of IoT. The new paradigm goes beyond traditional privacy risks.

- **Privacy must be balanced against the desire for innovation.**
- **With IoT connectivity is ubiquitous and the volume of data collected is risk itself**
  - Exposure of PII must be minimized
- **Beyond PII, the collection of related sensitive personal info raises additional concerns in a "sharing economy."**
  - Geolocation, financial information, health data, etc.
- **Lack of transparency around data policies and management can undermine consumer or constituent confidence**
- **Federal laws to protect consumer and government data, were conceived long before IoT. They include:**
  - The Privacy Act of 1974
  - Heath Insurance Portability and Accountability Act (HIPAA)
  - Computer Fraud Abuse Act (CFAA)
  - Electronic Communications Privacy Act (ECPA)

Challenge Area 3 - Managing IoT Risk

Understanding and managing the risks presented by IoT is a critical success factor

- **Disruption and denial of service**
  - Managing continuous availability across all devices required by the enterprise
- **Complexity of vulnerabilities**
  - Design with security in mind and incorporate pre-built, role-based security models
- **Vulnerability management**
  - Effective, timely patching on devices dependent on firmware upgrades
  - Managing default credentials and remote connect and management capabilities for IoT devices

Source: Seven IOT Risks You Must Consider by Ajay Kumar Information Security Insider Edition, Securing the Internet of Things, August 2014

Challenge Area 3 - Managing IoT Risk, continued

- **Identifying, implementing security controls**
  - Layer security and redundancy
  - Identify and implementing effective controls is up to the enterprise vs. the product developers
- **Fulfilling the need for security analytics capabilities**
  - Identify legitimate and malicious traffic patterns
  - Actionable threat intelligence measures critical for identifying malware
- **Modular hardware and software components**
  - Adopt security paradigm that isolates devices/embedded systems from the enterprise network
- **Rapid demand in bandwidth requirement**
  - Increased demand will proliferate business continuity risks

Slide Content: Courtesy MITRE

Case Study – Smart Buildings

GSA Link² project utilizes sensors to drive value with Smart Building Analytics.

- **Real time service delivery** – Utilize automated fault detection through building analytics to achieve organizational alignment in facilities management.
- **Service management** – Distribution of business model and allocation of resources to correct faults and save energy to deliver property management services better tomorrow.
- **Service planning** – Analytics can be utilized to consolidate facilities management to reduce the number of property managers and monitor and meter the core assets in the buildings.
- More information: http://www.gsa.gov/portal/category/100731

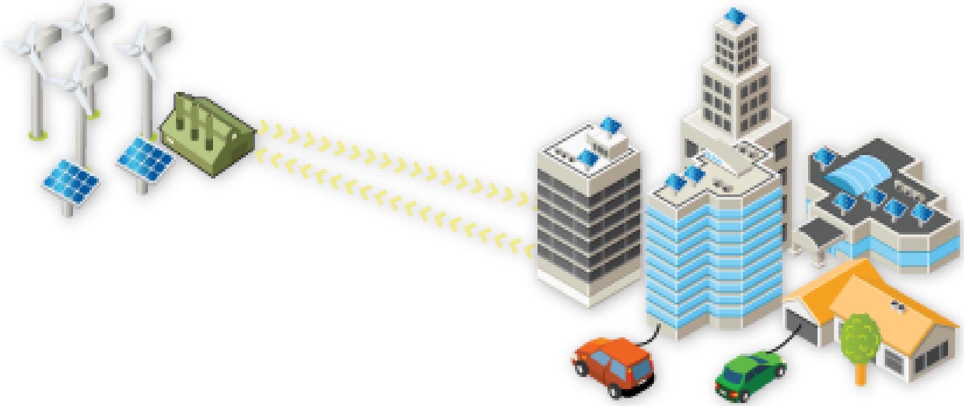


Image: Rocky Mountain Institute (www.rmi.org)

Case Study – Border Control

Slide Content: Courtesy MITRE

Ground sensors and radar on U.S. borders track, identify and classify illegal incursions through the use of seismic, magnetic, acoustic, IR imager and radar, etc.

- **Real time service delivery** – Utilize automated detection to notify border patrol agents of incursions.
- **Service management** – Distribution and reallocation of border control resources based on predictive analytics.
- **Service planning** – Analytics can be used to identify and classify types of vehicles and distinguishing various objects (e.g. groups of people, individuals, animals.
- More information: http://www.cbp.gov/border-security

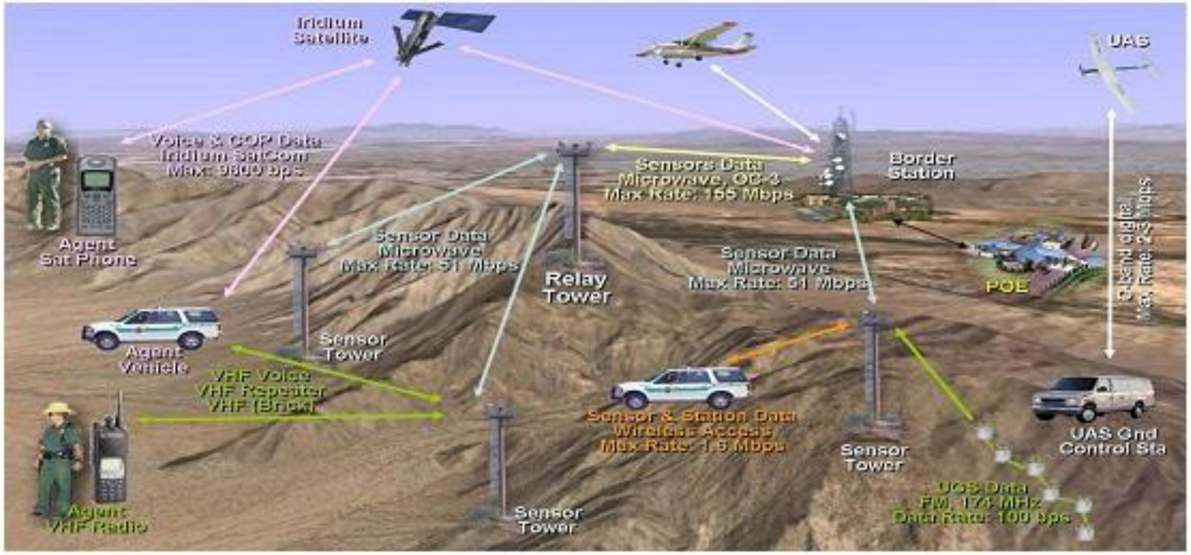


Image: US Customs and Border Protection

Recommendations

Recommendation 1: Embrace the opportunity

- IoT represents a smarter way of doing many of the things that government has been doing for years.
- Government must fully embrace the potential of IoT to improve the delivery of services and make government more efficient and effective.

Recommendation 2: Educate

- Government should embark on a mission to educate the general public and federal agencies on the benefits of IoT either through the development of a National Internet of Things Strategy or related policy.

Recommendation 3: Avoid unnecessary regulation

- Congress and the Executive Branch should avoid regulating the IoT in any manner that would serve to hinder the growth of or opportunity presented by IoT, instead focusing on promoting consensus based standards for IoT.

Recommendations, continued

Recommendation 4: Ensure privacy protections

- Government has a critical role to play in ensuring that personal information is protected and should embrace the challenge, while keeping privacy policies up-to-date to reflect the realities of a connected world.

Recommendation 5: Protect the IoT landscape

- The success or failure of IoT's application in government may hinge on the ability to secure all facets of the IoT channel, as every endpoint and network connection is a potential security risk. Government must promote policies that ensure the security of the IoT landscape and identify best practices, while encouraging technology development

Methodology

- Over the course of 10 weeks, beginning in July 2015, ATARC convened an Innovation Lab consisting of more than 20 representatives from government, industry, and academia. The IoT Innovation Lab was led by Linda Garcia of Cisco who served as Chair and Craig Ano of Samsung and Bryan Schromsky and Mohammad Rehman of Verizon who served as Vice Chairs.
- The group met 6 times to debate issues related to the application of the Internet of Things to government.
- The results of the findings are summarized in the preceding report.

Acknowledgements

Thanks to the following for their contributions and participation in the ATARC Internet of Things Innovation Lab.

- Linda Garcia, Cisco, Chair
- Craig Ano, Samsung, Vice Chair
- Bryan Schromsky, Verizon, Vice Chair
- Mohammad Rehman, Verizon, Vice Chair
- Tom Suder, ATARC
- Mike Hettinger, ATARC
- Tim Harvey, ATARC
- Karen Caraway, MITRE
- Nancy Ross, MITRE