



Policy Framework for the Internet of Things (IoT)

The IoT Transformation

The world is in the midst of a dramatic transformation from isolated systems to Internet-enabled devices that can network and communicate with each other and the cloud. Commonly referred to as the Internet of Things (IoT), this new reality is being driven by the convergence of increasingly connected devices, compute and data economics, and the proliferation and acceleration of cloud and big data analytics. This shift in technology is generating unprecedented opportunities for the US public and private sectors to develop new services, enhance productivity and efficiency, improve real-time decision making, solve critical societal problems, and develop new and innovative user experiences.

These transformational opportunities will significantly impact the entire marketplace across numerous sectors from manufacturing and transportation to utilities and healthcare – fueling GDP, creating new jobs, and bolstering the US economy. McKinsey Global Institute identifies the IoT as one of the most under-hyped technologies with great economic potential – on the scale of \$2.7 to \$6.2 trillion of estimated global economic impact in 2025 – with the US and other developed economies capturing 70 percent this economic impact.¹ Similarly, Cisco projects that, by 2022, the US alone has the opportunity, if the US demonstrates real leadership in this area, to capture 32 percent of the global “value at stake” in the IoT economy² – or approximately \$4.6 trillion. And GE estimates that the IoT could boost US average incomes by 25 to 40 percent over the next twenty years.³ Moreover, consumer demand for the IoT is high: Intel found that half of all Americans already desire a driverless society, support drones for public service or want cities to invest in

¹ *Disruptive Technologies: Advances that will transform life, business, and the global economy*, McKinsey Global Institute (May 2013), http://www.mckinsey.com/insights/business_technology/disruptive_technologies. Assessing a longer timeframe, GE estimates that, over the next 20 years, the Industrial Internet could add \$10-15T to global GDP. *Industrial Internet: Pushing the Boundaries of Minds and Machines*, GE Corp. (Nov. 2012) (“GE Report”), http://www.ge.com/docs/chapters/Industrial_Internet.pdf.

² Cisco projects that, from 2013-22, the US will capture 32% of the \$14.4T global “value at stake” in the IoE economy. *The IoE: Global Private Sector Market Analysis*, Cisco Corp. (2013), http://www.cisco.com/web/about/ac79/docs/innov/IoE_Economy_FAQ.pdf. Cisco also estimated that, in 2013, companies in the U.S. would realize only 53% of their potential \$473B IoE Value at Stake, leaving 47% on the table due to the need for further investments in foundational and cutting-edge IoE technologies and/or internal transformation through management best practices enabled by technology. *IoE Value Index*, Cisco Corp. (2013), http://internetofeverything.cisco.com/sites/default/files/docs/en/ioe-value-index_Whitepaper.pdf.

³ GE Report.



smart infrastructures that would use and apply non-personal data from cars and buildings to improve quality of life for them and their community.⁴

Intel and the IoT

To address immediate market demand for the IoT, Intel is focused on accelerating the development and deployment of intelligent devices, creating “systems of systems” by horizontally connecting the edge of IoT solutions to the cloud, and enabling end-to-end analytics to transform business. Among its many capabilities, a successful end-to-end strategy makes existing devices more intelligent and secure to reliably filter and manage data locally – so that they can seamlessly interact with each other as well as new devices and infrastructure. Intel technology drives these end-to-end strategies, powering devices from the edge of the network to the data center with industry leading hardware, software, and services, and the delivery of important user experiences such as device set up times. In order to reach IoT scale and deployment velocity, Intel developed the Intel® IoT Platform,⁵ an end-to-end architecture based on secure horizontal and interoperable building blocks that functions as an IoT platform that can be deployed across industry sectors. Utilizing our cutting-edge solutions, Intel will be the preeminent building block supplier for IoT deployments, and through partnerships with corporations and governments worldwide deploy cutting edge IoT solutions in sectors like manufacturing,⁶ utilities,⁷ healthcare,⁸ and public safety,⁹ and smart cities like London (Smart City/Infrastructure), Dublin (Smart City/Infrastructure), and Shanghai (Transportation).¹⁰

⁴ *The Vote Is In: Citizens Support 'Smart Cities' with Driverless Cars, Public Service Drones and Surroundings that Sense Activities*, Intel Corp. (Feb. 2014), http://newsroom.intel.com/community/intel_newsroom/blog/2014/02/10/the-vote-is-in-citizens-support-smart-cities-with-driverless-cars-public-service-drones-and-surroundings-that-sense-activities.

⁵ *Intel Unifies and Simplifies Connectivity, Security for IoT*, Intel Corp. (Dec. 2014), http://newsroom.intel.com/community/intel_newsroom/blog/2014/12/09/intel-unifies-and-simplifies-connectivity-security-for-iot.

⁶ Manufacturing: <http://www.intel.com/content/www/us/en/internet-of-things/videos/iot-in-action-video.html>

⁷ Utilities: <http://www.intel.com/content/www/us/en/intelligent-systems/iot/daikin-applied-transforms-hvac-with-iot.html> and <http://www.intel.com/content/www/us/en/energy/westfalen-weser-energie-relay-station-monitoring-vpro-xeon-case-study.html?wapkw=westfalen>

⁸ Healthcare: <http://www.intel.com/content/www/us/en/intelligent-systems/tech-today/careview-video.html?wapkw=healthcare+iot>

⁹ Public Safety: <http://www.intel.com/content/www/us/en/intelligent-systems/tech-today/big-data-analysis-improves-orange-county-emergency-response-video.html>

¹⁰ London: <http://www.intel.com/content/www/us/en/internet-of-things/smart-city-london.html>. Dublin: <http://www.siliconrepublic.com/innovation/item/36336-intel-to-turn-dublin-into-w>. Shanghai: <https://www.youtube.com/watch?v=MOZN8E16fY>.



This document sets forth Intel’s vision and goals for our country’s IoT ecosystem, as well as IoT policy principles regarding (i) connectivity and interoperability; (ii) privacy and security; (iii) intelligent analytics and big data; (iv) open standards; (v) data and device discoverability; and (vi) public-private partnerships.

IoT Vision and Goals

- A vibrant and state-of-the-art IoT ecosystem is critical to our nation’s global competitiveness and economic stability in the 21st century.
- The US government should work with industry to establish a long-term federal goal that America leads the world with IoT solutions, with short-term milestones to track the nation’s achievement.
- To maximize the potential of the US IoT ecosystem, our policy framework must envision a wide range of applications – from Mobile¹¹ to Home¹² to Industrial¹³ domains – recognizing that regulations, requirements, and technical solutions may not be one-size-fits-all.
- America’s public policy framework must encourage the development of a robust IoT ecosystem that promotes critical capabilities, including connectivity and interoperability, privacy and security, and intelligent analytics and big data.
- To accelerate and maintain the long term viability of the IoT, our policy framework should encourage solutions based on horizontal building blocks and an open architecture – one that is scalable, interoperable, and reusable across deployments, vendors, and sectors.
- Our nation’s public policy framework also should contemplate tools to accelerate IoT adoption and enable cost-effective introduction of new technologies, including open standards efforts, targeted federal funding, and impactful public-private partnerships.
- By understanding these fundamental building blocks of a successful IoT ecosystem, policymakers can enable the proliferation of these technologies across markets and help our nation realize the significant economic and societal benefits that the IoT can deliver.

¹¹ Examples of Mobile usage models include automobiles, wearables, and phone/tablet-based applications.

¹² Examples of Home usage models include home and building automation.

¹³ Examples of Industrial usage models include monitoring high-value industrial assets, transportation, and infrastructure, as well as facilitating manufacturing automation and energy grid automation.



Policy Principles

Connectivity and Interoperability

- IDC predicts 50 billion devices will be connected to the Internet by 2020.¹⁴
- Thus, connectivity is imperative for the US to realize the full power of the IoT; systems of intelligent devices (often called “systems of systems”) must be connected to each other or the network(s) in order for our nation to seize the maximum potential of our transformational IoT opportunities.
- However, as more than 85 percent of existing devices worldwide are based on unconnected legacy systems,¹⁵ it is critical that industry focuses on the development and deployment of solutions needed to address connectivity and interoperability of legacy devices as an interim step to avoid replacing all existing infrastructure and still realize the benefits IoT can deliver to this legacy environment.
- To address this connectivity and interoperability, our nation’s public policy framework must contemplate intelligent gateway solutions that can connect legacy systems and provide common interfaces and seamless communication between devices and the cloud.
- This approach to connecting legacy systems will accelerate the impact of the IoT by allowing data from existing infrastructure to be captured and utilized to immediately deliver value, while enabling legacy devices to seamlessly interact with each other and existing infrastructure as well as new devices and infrastructure that are later added to our IoT ecosystem.
- Our nation’s spectrum resource is an essential building block for IoT device connectivity. Ubiquitous, affordable, high-speed broadband connections over licensed and unlicensed airwaves are critical to enable consumers and the public and private sectors throughout the IoT ecosystem. Thus, effective and efficient management of this increasingly scarce resource must be a priority for policymakers as the US builds a thriving IoT ecosystem.

¹⁴ *Business Strategy: The Coming of Age of the "Internet of Things" in Government*, IDC (April 2013), <http://www.idc.com/getdoc.jsp?containerId=GIGM01V>.

¹⁵ IMS Research (July 2012).



Privacy and Security

- Privacy and security are critical building blocks for our nation’s IoT ecosystem – and capabilities that must be designed into our IoT systems from the outset using the best known Privacy-by-Design methodologies.¹⁶
- Therefore, to maximize the potential of a US IoT ecosystem that promotes Mobile, Home, and Industrial domains, our public policy framework must have a clear and implementable privacy and security strategy.
- This strategy must contemplate the range of purposes and risks among the various market applications, sectors, and domains, and create a logical and implementable framework that encourages industry innovation for appropriate solutions.
- For trusted data exchange in an IoT ecosystem, data generated by devices and existing infrastructure must be able to be shared between the cloud, the network, and intelligent devices for analysis – enabling users to aggregate, filter, and share data from the edge to the cloud with robust protection.
- Moreover, data must be accurate to be beneficial. So our nation’s public policy must promote the importance of accuracy and integrity of data in all market sectors, but especially in the industrial domain where the safeguarding of critical infrastructure can be vital to economic and social stability.
- Our nation’s public policy framework also must evoke consumer and industry trust through hardened privacy and security solutions in order to motivate adoption and participation in the IoT marketplace.
- The IoT presents new challenges for traditional privacy principles. Consumer notice and consent will continue to be important, however other privacy principles must also be emphasized to ensure consumer privacy is adequately protected. For example, focusing on accountability for the appropriate collection, use, and protection of the consumer’s data.
- Optimal privacy and security methods must be developed as required for different IoT solutions. Use cases should be used to proactively identify privacy and security risks and to develop robust strategies to mitigate those risks.

¹⁶ Privacy by Design (PbD) is a carefully managed process where products and services are proactively evaluated for potential privacy and security risks before and during product development. PbD promotes the development of effective strategies to integrate appropriate privacy and security protection into products and services to mitigate the identified risks.



Intelligent Analytics and Big Data

- Our nation's IoT policy framework must appreciate that analytics and the insights it provides will be the driving force to deliver IoT productivity and efficiency improvements, as well as new business/service opportunities, across both the public and private sectors.
- A successful IoT ecosystem will be designed by industry to unlock data intelligence from the device through the network to the cloud – enabling the government and businesses to provide better products and services and enriched consumer experiences.
- Therefore, America's IoT vision must include the development of horizontal building blocks for end-to-end analytics, as well as distributed analytics solutions for edge systems and the data center, which enable governments, businesses, and consumers to turn big data into actionable information.
- With this enormous volume of new data generated and shared across intelligent devices and systems that can now be analyzed, a wealth of untapped value can be extracted to increase economic efficiency and productivity across the US.

Open Standards

- A certain level of standardization and interoperability is necessary to achieve a successful, IoT ecosystem. In the emerging IoT economy, voluntary global standards can accelerate adoption, drive competition, and enable cost-effective introduction of new technologies.
- Furthermore, open standards which facilitate interoperability across the IoT ecosystem will stimulate industry innovation and provide a clearer technology evolution path.
- Industry is in the best position to develop the technological standards and solutions to address global IoT ecosystem opportunities and challenges. Government should encourage industry to collaborate in open participation global standardization efforts to develop technological best practices and standards.
- Specifically, government should encourage the use of commercially available solutions to accelerate innovation and adoption of IoT deployments. The emphasis on commercially available solutions and market-adopted voluntary standards will allow for faster adoption and increase innovation, bringing the IoT and its benefits to reality sooner.



Data and Device Discoverability

- Data created from existing devices, new devices, and “systems of systems” in IoT deployments must be able to be managed dynamically in a common way. The ability to categorize data as public or private and manage that data dynamically will allow for increased growth in single business, cross-business, and public sector implementations.
- In addition, as devices become connected, it will become critical that both the devices and the data that is being generated are able to be discovered by an application or sought out by service in a common manner to provide value. The ability to find devices and data will increase the pace of IoT solution deployment and the societal benefits that follow.
- For this reason, our nation’s IoT policy framework should encourage government and industry to work together to architect a common set of best methods to allow for device and data discoverability. The result should provide a robust data exchange solution that is easy to implement on both new and existing solutions.

Public-Private Partnerships

- Government and industry collaboration can be one of our nation’s best assets to accelerate the adoption of a world-class IoT ecosystem that successfully supports Mobile, Home, and Industrial domains.
- Viable public-private partnerships will make IoT deployments an appealing investment for government and industry, as well as ensure scalability and sustainability of infrastructure and technological innovation over the long term.
- Government and industry should work together to promote a business environment that motivates private investment and innovation – including the protection of commercial and proprietary data from misuse by competitors and third parties.
- Data ownership is a critical component to delivering economic value and must be defined between government, industry, and consumers. For example, in order to incentivize investment in America’s IoT ecosystem, it is essential that our public policy framework ensures protection of proprietary and commercial data that could be considered IP.
- Public-private partnerships should leverage existing industry standards and investments and utilize both public and private resources in order to facilitate the research, leadership, and governance to advance our nation’s IoT vision.



- Federal funding may be appropriate in certain targeted situations to incentivize more rapid development and deployment of our nation's IoT ecosystem.

* * *