CA TECHNOLOGIES | Business rewritten by software

The Benefits, Challenges, and Potential Roles for the U.S. Government in Fostering the Advancement of the Internet of Things

Prepared for:

National Telecommunications and Information Administration

U.S. Department of Commerce
1401 Constitution Avenue N.W., Room 4725
Attn: IoT RFC 2016
Washington, DC 20230

CA Technologies Point of Contact:
Brendan Peter
Vice President, Global Government Relations, CA, Inc.
Brendan.Peter@ca.com

607 14th St NW, Ste 660
Washington, DC 20005

June 2, 2016

U.S. Department of Commerce
1401 Constitution Avenue N.W., Room 4725
Attn: IoT RFC 2016
Washington, DC 20230
Via email: *iotrfc2016@ntia.doc.gov*

Reference: The Benefits, Challenges, Potential Roles for the U.S. Government in Fostering the Advancement of the Internet of Things

Dear Sir or Madam:

CA Technologies (CA) appreciates this opportunity to provide comments to the National Telecommunications and Information Administration (NTIA) on the potential benefits and challenges of Internet of Things (IoT) technologies and what role, if any, the U.S. Government should play in this area.

CA Technologies helps customers succeed in a future where every business is being rewritten by software. From planning to development to management to security, at CA we create software that fuels transformation for companies in the application economy.

CA Technologies is responding to this RFC as a provider of software solutions that help manage, analyze, and secure IoT technologies and as a global company familiar with the wide range of IoT regulatory and assessment approaches being pursued by governments around the world.

Our response to the RFI is provided in the enclosed attachment. We look forward to working with NTIA and other federal agencies on promoting adoption of IoT technologies, and in developing risk management-based security and privacy policies to build trust in the IoT. If you have any questions or comments about our submission, please feel free to contact me at brendan.peter@ca.com.

Sincerely,

Brendan Peter
Vice President, Global Government Relations
CA, Inc.

Table of Contents

Section 1: Introduction

The Internet of Things (IoT), and the data-driven innovation it promises, provide a wealth of opportunities for improving public health, increasing agricultural yields, generating and consuming energy more efficiently, protecting the environment, enhancing transportation safety and efficiency, strengthening manufacturing, and for improving countless other applications. It has the potential to impact nearly every single industry and business model in transformative ways. With the growth and deployment of the IoT, we are at the dawn of what Klaus Schwab, the Executive Chairman of the World Economic Forum has termed, "the Fourth Industrial Revolution."[1] At CA, we call this development "the Application Economy."

However, in addition to the range of opportunities that IoT offers, it also comes with significant technology and policy challenges. With more than 50 billion connected devices expected by 2020[2], organizations will need to be able to authenticate, secure, manage, analyze, and act on the wealth of data that will be generated.

Sensors and devices from different manufacturers will generate wide varieties of data at different velocities, will communicate with different back-end data processing and analytics systems, and will execute varied functions. Organizations will need to ensure that the devices themselves and the data they receive and interpret are authenticated, especially if the devices are programmed to execute actions based on this data. A significant percentage of these devices and sensors will be wireless and will require ubiquitous access to spectrum. And, because so much of the data generated by the IoT will be generated by and associated with people, personal privacy will need to be protected throughout the IoT lifecycle.

CA Technologies welcomes the opportunity to provide a response to the National Telecommunications and Information Administration Request for Comment on the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things.

CA Technologies makes software for businesses that are development-driven, because we believe those who build the apps will own the future. We help our customers succeed in a future where every business—from apparel to energy—is being rewritten by software. From planning to development to management to security, at CA we create software that fuels transformation for companies in the application economy. Our goal is to help organizations develop applications and experiences that excite, engage and open up new markets for their businesses. CA solutions power innovation by helping organizations to understand, plan, manage and control infrastructure to ensure the best possible business outcomes.

CA has structured its response by highlighting technology opportunities and challenges associated with the IoT, and by making recommendations for the Department of Commerce and other US Government officials in developing IoT policy.

[1] https://www.weforum.org/pages/the-fourth-industrial-revolution-by-klaus-schwab/
[2] http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

Section 2: IoT Technology Opportunities and Challenges

The Internet of Things (IoT) constitutes an extension of Information Technology (IT) from data centers and personal computing devices to everyday appliances and objects; from data servers and smart phones to internet-enabled smart vehicles and food packages that are tagged with beacons, Radio Frequency Identification (RFID) chips or Quick Response (QR) codes.

This extension creates significant opportunities for exchanging and monetizing information, conserving natural resources, and improving people's lives. The IoT will enable organizations to operate systems and supply chains more efficiently by generating actionable insights combined with automation and integration of business processes. IoT solutions also can enable the automation of dangerous or tedious activities (such as transport, mining, warehouse management, and property surveillance.)

This extension of traditional IT functions also introduces new challenges: it expands the cybersecurity attack surface, it exposes new privacy challenges, and it greatly increases the load on IT infrastructure and service support. CA Technologies highlights many of the technology challenges associated with IoT below.

Heterogeneity and lack of standards

There are many different types of sensors which provide multiple types of content over various protocols. There are currently dozens of competing platforms, though as profitable and significant use cases emerge, the field of IoT products will likely see some convergence over the next several years. In anticipation of this convergence, a number of consortia and open-source activities have designed and developed strong foundations. The Eclipse Foundation, for example, has well-articulated reference architecture and is supporting the development of components for an open-source IoT stack. At the same time, IBM, Google and Cisco have developed significant platforms for IoT applications, and companies like CA Technologies are creating platform-agnostic components. Notably, some IoT frameworks focus on local computation to achieve real-time responses, while most other frameworks focus on sending continuous data streams to "big" data lakes.

The Department of Commerce, through the National Institute of Standards and Technology (NIST), can play a convening role to help industry identify key use cases to facilitate convergence and industry maturity. The NIST Cyber-Physical Systems Public Working Group is helping to promote this convergence and should continue to receive active Federal Government support.

Data exchanges and commerce challenges

Data is an asset and like other assets it can be traded and sold, and data exchange must be based on trustworthy networks. IoT applications provide deeper insights in the behavior and preferences of individuals and organizations. For example, the GPS locations of individual traveling salespersons might be useful to restaurants and hotels, but the collective GPS data of salespersons from the same company might be useful to competitors. Thus, the exchange and sale of data must be carefully managed to protect corporate and individual data throughout the data supply chain (as the data moves from one device into the network). Privacy and data-use policies should be transparent and verifiable, and individuals and companies should be able to determine who has access to data and how it will be used.

New attack vectors and security challenges

IoT Edge devices (e.g., sensors, semi-autonomous vehicles and robots) often operate in the open, where they are potentially exposed to adversarial or careless actors (e.g., workers, customers, and pedestrians). This means that an IoT foundation must be designed with the assumption that attackers could potentially gain physical access to devices and that they can use this access to control other resources. Further, unlike traditional IT in which devices have continuous reliable access to power (and battery backup), battery exhaustion can be an attack vector in the IoT.

Unlike traditional IT components, edge devices are often not online. Wireless connectivity may be insufficient at times, or battery-preserving algorithms may require sleep cycles. This has several consequences: (1) for end-to-end security, the edge devices must enforce rigorous security controls even when offline, and must restrict and log the types of changes that can occur, (2) new methods must be created to quickly integrate, update, and de-provision edge-devices and users at scale, and (3) the system must be able to distinguish between distributed denial of service (DDOS) attacks and the sudden, but legitimate, activity of many edge-devices.

Further, there is significant fragmentation across IoT hardware and software stacks. In many ways, the user doesn't know the execution context of the edge device, which complicates the security aspects in your infrastructure in significant ways. Therefore, users require flexibility in their access management and the ability to change policies, often in an automated fashion, in order to handle the scale of devices and their fragmented nature.

Finally, as IoT technologies become more ubiquitous and control an increasing number of critical functions, authenticating the identity of "things" and data will become increasingly important. Organizations will require strict access controls for IT administrators and other privileged users to prevent and/or mitigate incidental or malicious insider attacks.

Application Programming Interface (API) management and security challenges

Increasingly, organizations will be making use of application programming interfaces (APIs), which enable these organizations to derive increased value from multiple inputs. The effective management and security of these APIs will be vital to the success of the Internet of Things, Big Data and Mobility.

APIs allow developers to create an open architecture for sharing functionality and data between applications. APIs are like windows into an application—a direct conduit that leads straight into the core functionality and data residing in the heart of the app. APIs will be critical to the interfaces between sensors, devices and applications in the emerging IoT ecosystem. Leveraging APIs and securing them will be vital in enhancing trust in the IoT.

APIs represent a great opportunity for the enterprise to integrate applications quickly and easily. But APIs can be a double-edged sword: promising agility, while at the same time increasing risk. Organizations will need to address API security as an architectural challenge long before any development takes place; if they can do so, the IoT will reap the rewards of this technological breakthrough safely and securely.

IT/IoT resilience challenges

IoT solutions often contain physical and software components manufactured and operated by multiple vendors. When something goes awry, it may be difficult to determine root cause and/or responsibility. This problem exists today – most web applications rely on coordinated activities of multi-vendor services and on cooperating operations analysts. However, IoT increases the scale of the problem not only because of the volume of data, but also because of the increase in the exposed attack surface. Service performance management and risk management must be optimized in a network where devices may have high failure rates, spurious data, and communication interruptions.

Inaccurate, but correctly formatted, data may appear throughout a network of sensors, and inappropriate actions may occur when robots or vehicles do not have all of the relevant environmental information. This may result in physical as well as financial damages, despite strong security. Autonomous IoT systems must rigorously verify data from the edge.

This suggests the need for:

- New methods for probing IoT infrastructure and for collecting, monitoring, analyzing, automating, and visualizing IoT data and data provenance;
- IoT frameworks that support agile application development and deployment by third parties and fast recovery/adaption when service intrusions/interruptions occur;
- Post deployment update capabilities without the need to replace hardware; and
- Forensics capabilities for determining and apportioning accountability.

Section 3: Policy Recommendations

CA Technologies evaluates proposed IoT policy initiatives through the lens of whether the policies will enable innovation, promote competition, enhance security and protect privacy in global markets. CA believes the following policy principles will be critical to the success of IoT development:

- Stakeholder engagement;
- Flexible, outcomes-focused policy;
- Recognition of global contexts in policy development;
- Infrastructure support; and
- Support for research and development and STEM education.

Stakeholder Engagement

Governments should engage actively with private and public stakeholders in developing IoT policies. Stakeholder engagement ensures that different technology development, management, security and privacy perspectives are weighed in policy development, and it encourages greater stakeholder participation and buy-in when policies are implemented. Effective public private partnerships can help promote IoT development, security and privacy while allowing for technology innovation.

The NIST Cyber-Physical Systems Public Working Group is a good example of an effective public private partnership, and is currently working to develop consensus definitions, reference architectures, and common lexicon for IoT. The US Government should continue to support active stakeholder engagement initiatives such as this group.

In addition, the US Government should promote global, industry-led, market-driven standards development. Global, industry-led standards development processes best reflect technology developments and establish common baselines above which technology providers can compete and innovate. In cases where multi-lateral (state-based) standards bodies work to develop IoT standards, the US Government and the US Department of Commerce should work closely with industry and organizational stakeholders to promote existing industry-led standards when possible.

Flexible, outcomes-based policy

Policy and regulatory flexibility will be increasingly important in the development of the IoT. Each industry, system, and business faces distinct IoT challenges, and the range of stakeholders must have flexibility to uniquely address their needs. CA supports technology-neutral, outcomes-based policies that enable stakeholders to choose from a variety of options to address their development, management, security, and privacy challenges, and opposes policies that impose specific technology mandates.

The NIST Framework for Improving Critical Infrastructure Cybersecurity allows for flexibility in cybersecurity approaches among critical infrastructure providers, based on their unique threat environments, priorities and risk management approaches. CA believes similar policy approaches, which incorporate flexibility and which allow organizations to select their own, appropriate security and privacy options to achieve outcomes, will be critical for the IoT, given its vast range of technologies, functions and systems.

Recognition of global contexts in policy development

There is significant risk that global governments and US Federal regulatory agencies will develop multiple, distinct and overlapping compliance regimes around the IoT. This policy fragmentation can lead to organizations dedicating scarce resources towards compliance exercises and away from innovation and development. The Department of Commerce can help lead inter-agency IoT policy alignment initiatives, and can also work with global partners to promote policy alignment, where possible.

CA Technologies also believes that policy makers should embrace international, market-driven standards rather than country-specific technology mandates for the IoT. International standards are vital to vendors' ability to deliver secure, resilient and cost effective solutions that meet truly global performance requirements. Local standards fracture markets, increase cost and may weaken security

Further, CA Technologies believes that the imposition of restrictions on where products can be developed or where data can be stored as a condition of market access, for example, will stifle innovation and limit customers' ability to buy the most effective and secure IoT solutions to address their needs, limiting the potential benefits to consumers and society.

Infrastructure support

The explosive growth of internet-connected devices and automated data analytics systems will require much more robust internet infrastructure. The government should continue to promote strong broadband deployment. The US Government should also continue to open up broadband spectrum for licensed and unlicensed use. And the government should support research efforts on spectrum sharing capabilities and technologies.

Support for Research and Development and STEM Education

To fully realize the myriad economic and social benefits of the IoT and the application economy, public policy makers should support the scientific and technical foundations which provide a basis for private sector innovation by prioritizing funding for research and development at universities, research institutes and national laboratories.

The Networking and Information Technology Research and Development (NITRD) program includes research on data analytics and cyber physical systems. Multi-disciplinary research programs, such as the NITRD program will be increasingly important for the continued development of the Internet of Things.

The IoT and the application economy will present a vast array of opportunities for innovators to develop new products and services to improve people's lives. Getting students excited about these opportunities and the educational backgrounds necessary to succeed in these ventures will help us realize these potential benefits.

CA believes policy makers must promote strong benchmarked math and science standards for all K-12 students. In our increasingly global economy, it is imperative that students around the world are equipped with the right set of skills and problem solving capabilities that will help them lead the digital economy of the future. Further, given the increasing prevalence of information technology in the economy and in our society, it is imperative that students receive instruction in basic coding and other ICT fields.

Conclusion

The burgeoning Application Economy and the IoT provide significant opportunities to strengthen global economies and improve quality of life.   However, we will not be able to maximize the benefits of digital transformation unless there is strong user and organizational trust in IoT technologies. This trust must be supported by efficient, flexible, risk management-based government policies, developed in coordination with global stakeholders. CA Technologies appreciates NTIA's efforts in identifying the appropriate role for government policy to play in fostering the development of the Internet of Things. We look forward to continued engagement with NTIA and the Department of Commerce, global industry, and other key stakeholders as we work together to promote the IoT.