The Software Alliance

BSA

January 17, 2017

Secretary Maximiliano Salvadori Martinhão
Informatics Policy Office
Ministry of Science, Technology, Innovation, and Communications

Re: Public Consultation – National Internet of Things Plan

Dear Secretary Martinhão,

BSA | The Software Alliance ("BSA")[1] is thankful for the opportunity to contribute to the Ministry of Science, Technology, Innovation, and Communications (MCTIC)'s public consultation (Consultation) on the main aspects to be taken into account for the development of the Internet of Things (IoT) in Brazil.[2] As the leading global advocate for the software industry, BSA has a keen interest in this consultation and is hopeful that it will aid in the development of a national strategy for leveraging the full potential of IoT and its underlying technologies.

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

BSA's members include: Adobe, ANSYS, Apple, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, DataStax, IBM, Intuit, Microsoft, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, Trimble Solutions Corporation, The MathWorks, Trend Micro and Workday.

[2] Public Consultation available at http://www.participa.br/cpiot/itens-da-consulta

We, therefore, submit the contribution below for consideration and look forward to continue participating in this important discussion. We stand ready to answer any questions you may have about this submission.

Best regards,

Antonio Eduardo Mendes da Silva
Brazil Country Manager

Introduction

"Internet of Things" (or "IoT"), as the Consultation duly notes, consists of a very broad ecosystem. IoT is an umbrella term for a broad set of technologies and supporting services that collectively have the potential to transform virtually every facet of modern life. BSA members are on the leading edge of developing these new network-connected technologies that leverage data in an unprecedented way.

Given the broad set of underlying technologies and endless potential use cases that are implicated IoT, a one-size-fits-all approach to regulation would be counterproductive. We are, therefore, pleased by MCTIC's decision to undertake a holistic, ecosystem-wide evaluation of the opportunities and risks posed by the Internet of Things through a study to be conducted by the Brazilian Development Bank (Banco Nacional para o Desenvolvimento – "BNDES") which will take into account the input gathered through this Consultation. We also applaud MCTIC's intention to continue working with stakeholders to develop and implement an IoT plan for Brazil after the study is concluded.

As detailed below, the growth of the Internet of Things presents incredible opportunities for all segments of the Brazilian economy. In order to realize the full beneficial potential of these data-driven technologies, however, the public must trust the digital devices and services upon which the IoT is built. Establishing such a foundation of trust requires transparency, security, and predictability. For instance, technology providers must ensure that the public understands what data is being collected, how that data will be used, and that it will be secured using the best available technologies. At the same time, the Brazilian government must implement balanced privacy and cybersecurity regimes that protect consumers without hampering innovation and the power of the digital economy.

In addition, we offer suggestions in these comments for future work streams that would foster IoT innovation and growth:

- To eliminate trade barriers that impact technology providers and negatively impact the ability to leverage IoT benefits, the Brazilian government should implement policies that are conducive to cross-border data flows and that encourage the adoption of open, voluntary and consensus-based international standards. In addition, public procurement policies should focus on whether a product or service best meets the needs at hand and provides good value for money, rather than on ancillary issues such as national origin or particular development and licensing models.

- To help the Brazilian government become an early adopter of IoT, we urge the upcoming study to be conducted by BNDES to evaluate how IoT can be leveraged to increase Federal, State, and Municipal government agencies' efficiency, improving the quality of public services, and reduce long-term government spending.
- To ensure that Brazil becomes an attractive location for IoT-related research and development, MCTIC should work with other agencies to help to promote workforce development policies that train the next generation of innovators.

Internet of Things and the Data Economy

The "Internet of Things" describes the growing network of "smart" devices that are embedded with Internet-connected sensors and that leverage cloud-based analytics that make the data actionable. Unlike Internet-connected devices that have been around for decades, advances in technology now enable "devices of all kinds – including smartphones, wearables, appliances, medical equipment, and vehicles – to connect with the Internet and each other to create, share and analyze information, all without human intervention."[3] These software-enabled devices use sensors to collect large volumes of data that can be stored and processed in the cloud to increase automation, improve efficiency, bolster performance, and add functionality to product and service offerings.

The promise of the Internet of Things lies in the data it receives and produces and in the technologies that transform that raw data into actionable intelligence. Economists estimate that companies investing in technologies to make better use of data will benefit from a "data dividend" of $1.6 trillion in the next few years and that data-enabled efficiency gains could add almost $15 trillion to global GDP by 2030.[4] Unsurprisingly, 90 percent of today's business leaders cite data as a key resource and fundamental business differentiator, on par with basic resources like land, labor, and capital.[5]

[3] Deloitte, *The Internet of Things Ecosystem: Unlocking the Business Value of Connected Devices* 5 (2014), available in English at http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/gx-tmt-Iotecosystem.pdf

[4] BSA | The Software Alliance, *What's the Big Deal With Data?* (2015), available in English (original) at http://data.bsa.org/wp-content/uploads/2015/12/bsadatastudy_en.pdf and in Portuguese (translation) at http://data.bsa.org/wp-content/uploads/2015/10/BSADataStudy_br.pdf

[5] Economist Intelligence Unit, *The Deciding Factor: Big Data & Decision Making*, Cap Gemini, 2012, *available at* https://www.capgemini.com/resources/the-deciding-factor-big-data-decision-making.

Companies in every segment of the economy are therefore quickly developing IoT strategies to improve their processes for gathering, storing, securing, analyzing and acting upon data. Consumers now have access to a range of IoT products that provide unique insights to improve their daily lives. For instance, a variety of "smart home" devices now enable consumers to automate daily tasks and reduce their energy consumption. And, new automobiles are equipped with more than 10 million lines of software code to control sensors that generate up to 25 gigabytes of data per hour that can be processed to enable safety and crash avoidance systems, reduce congestion, and route traffic more efficiently.[6]

Here are just a few other examples of how data is enabling progress and revolutionizing the way we live[7]:

- Increasing Farming Yields. Farmers in many countries, including Brazil, are using data from seeds, satellites, sensors, and tractors to make better decisions about what to grow, when to plant, how to track food freshness from farm to fork, and how to adapt to changing climates.
- Building Smart Cities. Barcelona is harnessing data to give city officials the ability to examine traffic patterns, analyze where to put public bike stations, and identify which areas of the city need more ATMs.
- Designing Energy-Efficient Buildings. In the United Arab Emirates, engineers are using new data tools to design the world's first positive-energy building that actually produces more energy than it consumes.
- Reducing Commute Times. The city of Stockholm partnered to install 1,600 GPS systems in taxis. Streaming software analyzes the data collected from these devices to provide insights on traffic flow, travel times, and optimal commuting routes. Travel times in Stockholm have already been reduced by 50 percent, and automotive emissions have been reduced by 10 percent.
- Fighting Disease. In Kenya, doctors are using mobile data to identify malaria patterns and locate hotspots that guide government eradication efforts.

From these examples alone, it's not surprising that developing countries are actually gaining ground faster than you may think when it comes to technological data and innovation. This represents a tremendous opportunity for Brazil.

[6] BSA, *What's the Big Deal With Big Data?*, p. 15

[7] Id

By 2020, analysts predict that there will be more than 50 billion IoT devices relied upon by consumers, governments and businesses.[8] While consumer-facing IoT devices have understandably drawn much of the attention, commercial and industrial sector applications are likely to account for upwards of 70 percent of the data-added value enabled by the Internet of Things.[9] For instance, during transcontinental flights, the sensors on a commercial aircraft's engines, flaps and landing gear can generate half a terabyte of data that is used to improve flight performance, reduce turbulence, and identify possible engine defects before they impact mission critical systems.[10] Telematic sensors in tens of thousands of delivery vehicles track engine performance, improve routing, and reduce fuel consumption and overall emissions.[11] And, cities are using sensors embedded in critical infrastructure to improve the efficiency of their resource management, public health, and transportation systems. Experts forecast that these types of IoT smart city initiatives will have an economic impact of up $1.6 trillion per year by 2025.[12]

Consumer Trust and the Data Economy

Data innovation is not only transforming how we interact with the world around us, it is also fueling a powerful new job-creation engine and potent job-force multiplier. For every data-related IT job created, another three jobs are estimated to be created for people outside of IT.

Fully capitalizing on the promise of the new data economy, however, requires a foundation of trust. Enterprises, governments and consumers will take advantage of the convenience and efficiencies of the Internet of Things only to the extent that they can trust the underlying technologies that are making use of their data. They will want to ensure that their data is kept both private and secure.

Of course, the balance of this trust equation will vary significantly depending on the particular nature of the IoT application in question. For instance, unlike certain consumer-facing devices, enterprise and industrial uses of IoT for things like predictive maintenance of equipment, automation of HVAC and lighting control systems, and transportation fleet management involve little, if any, personal

[8] *See* Valerio, Pablo, *Internet of Things: 50 Billion Is Only the Beginning*, EE Times, Feb. 28, 2014, http://www.eetimes.com/document.asp?doc_id=1321229

[9] *See*, McKinsey Global Institute, *The Internet of Things: Mapping the Value Beyond the Hype*, at i (June 2015).

[10] BSA, *What's the Big Deal With Big Data?*, p. 8.

[11] BSA, What's the Big Deal With Big Data?, p. 8.

[12] McKinsey Global Institute, *The Internet of Things: Mapping the Value Beyond the Hype*, at 5 (June 2015).

information and therefore present fewer privacy risks. At the same time, IoT technologies that do not involve the collection of personal information, may nonetheless present heightened security concerns. The point is that the range of policy considerations implicated by the Internet of Things will inherently vary based on the risk profile of individual use cases.

While each use case presents unique considerations, the following principles should serve as touchstones as industry and government work together to foster a foundation of trust to encourage continued IoT innovation:

I – Privacy and Transparency

The ability to transfer data internationally is key for the development of IoT. Brazil should implement a privacy framework that will allow companies to easily and responsibly transfer data internationally. It is paramount that Brazilian government implement balanced privacy regime that protects consumers without hampering innovation and the power of the digital economy.

Members of BSA have a deep and long-standing commitment to protecting consumers' personal data across technologies and business models as they recognize that consumers are only comfortable taking advantage of the benefits of new technologies if they trust that they will not lose control over their personal data. However, as noted above, enterprise and industrial uses of IoT in many instances involve non-personal data and, therefore, policy frameworks should refrain from applying the same rules to all types of data. Applying very stringent legal obligations to a broad range of data, regardless of its context and the actual potential for harm to the user is likely to have a chilling effect on the data driven innovation in Brazil negatively impacting economic growth. Data should only be deemed "personal" if it refers to a directly or indirectly identified or identifiable natural person.

Transparency is critical to the trust equation. Companies that provide or use IoT systems must ensure that the public understands the type and volume of data that an IoT device is collecting and how that data will be used. Transparency regarding the collection of personally identifiable information is particularly critical for purposes of establishing user consent. The ideal method for providing users with notice will vary based on the manner in which the public interacts with a particular IoT technology. While on-screen disclosures may be possible in some instances, use of QR Codes, online notices, or other methods reasonably designed to provide notice will also serve an important role building trust.

In today's world, a large amount of data is created through individuals' interactions with internet connected devices and express consent is not suitable in all instances. While we recognize that the data subject's consent can be a valid way of legitimizing the treatment of personal data, it should not be the only one. Allowing for a wide range of mechanisms for consent is even more important considering the advent of the IoT and the resulting data that can be analyzed and used to create societal and economic benefits.

In practical terms, it may not be feasible for an individual to provide consent in every situation. In certain circumstances, providing consent to legitimize every instance of data collection and treatment would be extremely burdensome for data subjects and could also prevent them from benefiting from new technologies[13]. For example, if an individual had to provide express consent to allow the data it generates every time he swipes his public transportation card into an electronic gate when entering and exiting the transportation public system, research based on the analysis of the data in conjunction with the data generated by other users to improve public transportation services could be severely impaired. If Brazil relies solely on express consent as a legal basis for processing, it risks not being able to leverage all the benefits of the data economy.

Other lawful basis for treating data, such as legitimate interest, should also be accepted. In reality, the legitimate interest legal basis for agents serves a particularly important role, where it may not be suitable or appropriate for either the owner or the responsible person to obtain consent to legitimize data collection and treatment or where it is premature to enter into a contract with a consumer. The legitimate business interest as a basis for processing data has become even more important in the advent of big data analytic and the Internet of Things. Considering legitimate business interest as an appropriate basis for treatment will allow new businesses based on data analytic to flourish in Brazil.

BSA urges the Brazilian government to continue a dialogue with all stakeholders on this important issue before the Data Protection Bill, currently pending Congressional approval, is finalized.

II – Security

Companies that provide or use IoT systems must also ensure that they are securing data and operation of their devices using the best available technologies. Security and

[13] The Future of Privacy Forum, "An Updated Privacy Paradigm for the Internet of Things" (2013), available in English at https://fpf.org/wp-content/uploads/Wolf-and-Polonetsky-An-Updated-Privacy-Paradigm-for-the-%E2%80%9CInternet-of-Things%E2%80%9D-11-19-2013.pdf

privacy protections should be commensurate with the sensitivity of the data being collected and the device’s potential risk profile. And companies must have the flexibility to continue to develop and implement new security technologies as they evolve. For example, encryption is an important tool for securing personally identifiable data in transit and at rest, and for maintaining authentication credentials to prevent bad actors from using IoT endpoints as gateways for broader network access.[14]

Furthermore, regulations should not prohibit or require the acquisition or deployment of specific products or technologies, including specific hardware or software. Entities responsible for data seek to protect a wide spectrum of targets against a wide variety of potential threats. Policies targeted at protecting information should enable the implementation of security measures that are most appropriate to mitigating the specific risks each company faces to increase effectiveness. Technology neutrality is important to ensure this objective is achieved.

Finally, it is also important to highlight that to enable a trusted device world, the private sector, technology users, and governments alike all have a shared responsibility for adopting best practices, enabling risk appropriate security measures.

- **Companies should incorporate security as they design IoT devices.** Every new IOT start up should begin by thinking about security from day one. Developers should employ a secure systems engineering approach when they architect new IoT systems, and apply technologies that are commensurate with devices potential risk profile. They should also ensure device software is updatable, and prevent the use of hardcoded default passwords. Many companies are already doing this. They are also already implementing a layered security model that takes advantage of technologies capable of defending IoT assets at the network layer, the application layer, in the cloud, in the device itself, and at the human interface layer.
- **Users must become informed and engaged.** In the same way that a growing number of computer users now understand the importance of basic computer hygiene like keeping software patched, using up to date anti-virus software, and refraining from clicking on unknown attachments; device users similarly need to take proactive steps to ensure good device security. These include changing a device’s default username and password when it is installed, ensuring that the software embedded in the device called firmware is kept up

[14] See BSA | The Software Alliance, Encryption: Security Our Data, Security Our Lives (2016), available in English at http://encryption.bsa.org

to date, and keeping authentication keys and the networks they run on secured. Companies deploying IoT devices in a commercial setting should also develop a rigorous and in-depth security strategy that includes a risk-management framework and takes advantage of best practices such as NIST's cybersecurity framework – as they should for their traditional IT infrastructure.

- **Policymakers can boost security breakthroughs and the agility to address evolving threats.** Policymakers have an important role in continuing to advance good device security by 1) investing in the long term R&D that can keep us one step ahead of bad actors, and 2) by ensuring that companies have the flexibility to develop new security technologies that meet changing threats without constraining or potentially duplicative technology mandates. Brazil can also play an important leadership role adopting and highlighting global, industry developed security best practices that can be used in developing a risk-management framework.

III - Regulatory Affairs

Considering IoT encompasses a broad range of technologies, business models, and use cases, governments must resist the temptation to pursue a one-size-fits-all approach to regulation. In most cases, existing legal regimes have proven sufficiently flexible in addressing new issues raised by emerging devices and online services without the need to tailor new legislation that may produce unintended consequences or add new burdens.

IoT remains in an early stage of development. In some areas, limited government regulations are appropriate, for example to establish data privacy and cybersecurity frameworks. In such cases, it is important for the Government of Brazil to keep such regulations in line with emerging international trends and best practices. An overly-regulated approach is likely to inhibit development, deployment and growth of cloud computing services, to the detriment of Brazilian businesses and other entities.

Despite IoT's early stage of growth, significant efforts and progress in developing industry standards and best practices has been achieved. For example, in 2014, the United States' National Institute of Standards (NIST) published a voluntary Framework for Improving Critical Infrastructure Cybersecurity[15], which was created with the input of stakeholders and that has been widely adopted by industries from various sectors. Although the framework was not designed specifically for IoT, the

[15] NIST's Framework for Improving Critical Infrastructure Cybersecurity available at https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

best practices the NIST Cybersecurity lays out can be applied to IoT. As the Government of Brazil seeks to establish an enabling policy environment to promote IoT, we urge MCTIC and other relevant agencies to work together and, where possible, look to industry best practices rather than formal regulations.

IV - Coordination and Predictability:

As the Government of Brazil develops and implements policies to foster the adoption of IoT, it is paramount that MCTIC and other Brazilian government agencies take a coordinated approach and provide clear and predictable indications to the market on the policies to be adopted and the objectives such policies seek to achieve.

In line with what MCTIC has done with this Consultation, it is also critical that the Government of Brazil continue to seek the input of interested and relevant private sector stakeholders to inform policy making in this area. This will allow investors to plan and execute long term strategies and investments in the Brazilian market and will help ensure that Brazil is positioned to become a global leader in developing an effective, trusted, transparent and restrained regulatory environment, that works well with emerging international practices, and allows Brazilian businesses and consumers to fully benefit from existing and future opportunities presented by IoT and related services.

MCTIC's Initiatives to Promote IoT Innovation

Consistent with the objectives of this Consultation, leadership from the MCTIC on the following initiatives could have a meaningful impact on IoT innovation and growth:

Encouraging Brazilian Government Adoption of IoT: As noted above, adoption of IoT could result in a great economic impact. The study that MCTIC has been recently commissioned and that will be conducted by BNDES should determine how IoT technologies can be used by federal, state and local governments to increase government efficiency, improve the quality of government services and reduce long-term government spending. The Brazilian government should also explore whether public-private partnerships can be leveraged to help finance long-term capital intensive infrastructure projects.

Engaging with other Brazilian Government Agencies to Eliminate Trade Barriers: MCTIC should engage with other Brazilian government agencies to promote policies that are consistent with a free and open global Internet.

- Barriers to **cross-border data flows**, including requirements for data to be stored in local facilities, undermine the enormous efficiencies of scale and economic benefits that accrue from data innovation and should be avoided.
- Intelligent devices must be connected to each other, and the cloud, often across geographic boundaries, to gain the network effects that is at the core of the opportunity chain. By avoiding the potential creation of connected device silos that are unable to talk to each other, governments should **encourage the development and use of interoperable, voluntary, consensus-based global standards**. Policies that rely upon voluntary, consensus-based global standards can help ensure that devices can be designed to high-standards once, and then mass produced in the most affordable ways to all sectors and all regions of the global economy.
- Brazil should **refrain from granting public procurement preferences** based on national origin or particular development and licensing models. Rather, procurement policies should be based on a cost/benefit analysis to allow government agencies to best accomplish their goals.

Promoting Workforce Development: MCTIC should help develop a national strategy for ensuring that Brazilian workers have the skills necessary to thrive in the new data economy. A consistent and skilled flow of computer science graduates will enable innovation to flourish in Brazil. While goods manufacturing is still very important for Brazil, innovation will be the force that will foster the development of economies around the globe. A robust strategy by the Federal Government is necessary to boost efforts to foster education in the STEM fields like computer science and software engineering. This will help close the skills gap, meet growing demand for computing jobs, and boost Brazil’s ability to compete and innovate.

Once again, we thank for the opportunity to share our views on these important issues. We stand ready to answer any questions you may have about this submission and we look forward to continue contributing to this dialogue.