Making smart cities and IoT a reality in Latin America:

a quick guide for decision-makers

About the GSMA

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with over 350 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces the industry-leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional conferences.

FOR MORE INFORMATION, PLEASE VISIT THE GSMA CORPORATE WEBSITE AT WWW.GSMA.COM.
FOLLOW THE GSMA ON TWITTER: @GSMA.

AUTHORS

Philipe Moura
Senior Regulatory Manager, Latin America | Government & Regulatory Affairs | GSMA

Stefano Nicoletti
Policy Director - Technology Policy | Regulatory Affairs | GSMA

EXECUTIVE SUMMARY

- The Internet of Things brings about an enormous opportunity for Latin America. The total revenue opportunity for the region by 2023 is USD 33 billion, according to GSMA Intelligence. However, the overall impact on GDP is likely to be a lot more substantial. For Brazil alone, McKinsey forecasts the impact of IoT by 2020 to be of at least USD 50 billion in the country's GDP.

- IoT solutions will innovate across a great variety of industries, such as energy, healthcare and transportation. They will combine communication networks and existing "off-line" services increasing productivity, diminishing waste and improving citizens' wellbeing. If governments and policymakers in Latin America want to realize the full benefits of the IoT and help close the technology gap between the region and developed countries they should take action, they should:

  - » Resist the temptation to consider IoT services as traditional telecom services. Legacy regulation – that is, regulations established long before the IoT became a reality to deal with traditional voice and data services, will be most often irrelevant, will unnecessarily stifle IoT innovation, slow down take up and ultimately damage consumer and business in the region

  - » Facilitate a cross-regulator, cross- department dialogue and strategy across the various government administrations. For example, utility and telecom regulators should define and work together on how to promote smart meters; Transport and Communication ministries should define together how communication networks will serve roads; Smart city planners from different towns should work together to define best practice and work on common standards.

- **A 3-STEP PLAN.** To design an IoT policy, policymakers should first build a 3-step plan consisting of scoping the country's needs and potentials, estimating the positive impact on different economic areas and IoT verticals, and then designing and implementing specific actions to enable such growth.

- **GOVERNMENT AS DEMAND ENABLERS.** Governments should consider their potential as demand enablers, and, where possible, migrate towards utilizing IoT-enabled solution for public services – from utilities to urban mobility and healthcare). Developing PPPs and seeking/offering various sources of funding can be an important step to secure this goal.

- **INTERNATIONAL STANDARDS AND BEST PRACTICES.** In considering challenges such as privacy, security, and standardization, governments should resist the temptation to create specific rules and national standards for IoT.

  - » A general data protection law that applies horizontally to all industries and services – not just IoT – is an important measure to secure trust in the IoT and guarantee consistent levels of protection for users.

  - » On what concerns security, it is important that governments support industry-led best practices and standards, which are constantly evolving to overcome threats, making it quicker and more cost-effective to adapt than rigid national standards.

  - » Governments should also note the myriad of efforts already being pursued by industry-led standards, and their importance for interoperability of services at the national and international levels – therefore, creating national standards would likely be counterproductive.

  - » A flexible and reliable governance structure. At the city level, it is important that mayors create a flexible governance model with an independent leader (such as a Chief Information Officer, CIO). For municipal services, mayors should always prefer scalable and interoperable solutions to avoid vendor lock-in. Finally, mayors should consider adopting open data policies to foster a data-enabled economy that could be easily used by citizens, NGOs and commercial entities. As well as providing one-stop access to a city's information, sharing data would support communication and analysis, more transparent and efficient policymaking, and create value by catalysing the development of innovative apps and services.

1. AN INTRODUCTION TO THE INTERNET OF THINGS

The Internet of Things (IoT) stands as one of the hottest topics in many industries and countries in Latin America, which have started to realise the many possibilities and benefits that can be brought about by a more connect world. From connected vehicles to fully automated manufacturing to real-time monitoring and decision-making in farms, the IoT can accelerate innovation and the growth of productivity. In fact, IoT is one of the key enablers for the upcoming productivity revolution on industry and services.

The positive impact of the IoT on citizens, consumers, businesses and governments will include improving individual health and well-being, helping governments provide better infrastructure and reduce healthcare and other costs, supporting overall reductions in carbon footprints, increasing access to education and other public services, and improving transportation safety and energy efficiency. For its positive impact alone, the IoT should be a top of mind subject for policymakers. GSMA Intelligence forecasts that there will be more than 1.3 billion IoT connections in Latin America by 2025 (see figure 1 below).

According to Machina, the total revenue opportunity for Latin America by 2023 is USD 176 billion, out of which USD 82 billion will be the application itself (three per cent or USD 5 billion of which would correspond to connectivity), and USD 94 billion will refer to the services that can be generated in relation to that application, such as data monetisation, system integration, and middleware replacement. In the case of Brazil, McKinsey forecasts the impact of IoT by 2020 to be of at least USD 50 billion in the Brazilian GDP alone.[1] Beyond the direct economic impact and revenue generation, IoT, as most telecommunication services, can generate much larger impact on the wider economy.

1. https://www.bndes.gov.br/wps/wcm/connect/site/269bc780-8cdb-4b9b-a297-53955103d4c5/relatorio-final-planodea-cao-produto-8.pdf?MOD=AJPERES&CVID=lXysvoX-&CVID=lXysvoX&CVID=lXysvoX&CVID=lXysvoX-&CVID=lXysvoX&CVID=lXysvoX

Figure 1: Total IoT Connections in Latin America, 2010-2025
Source: GSMA Intelligence

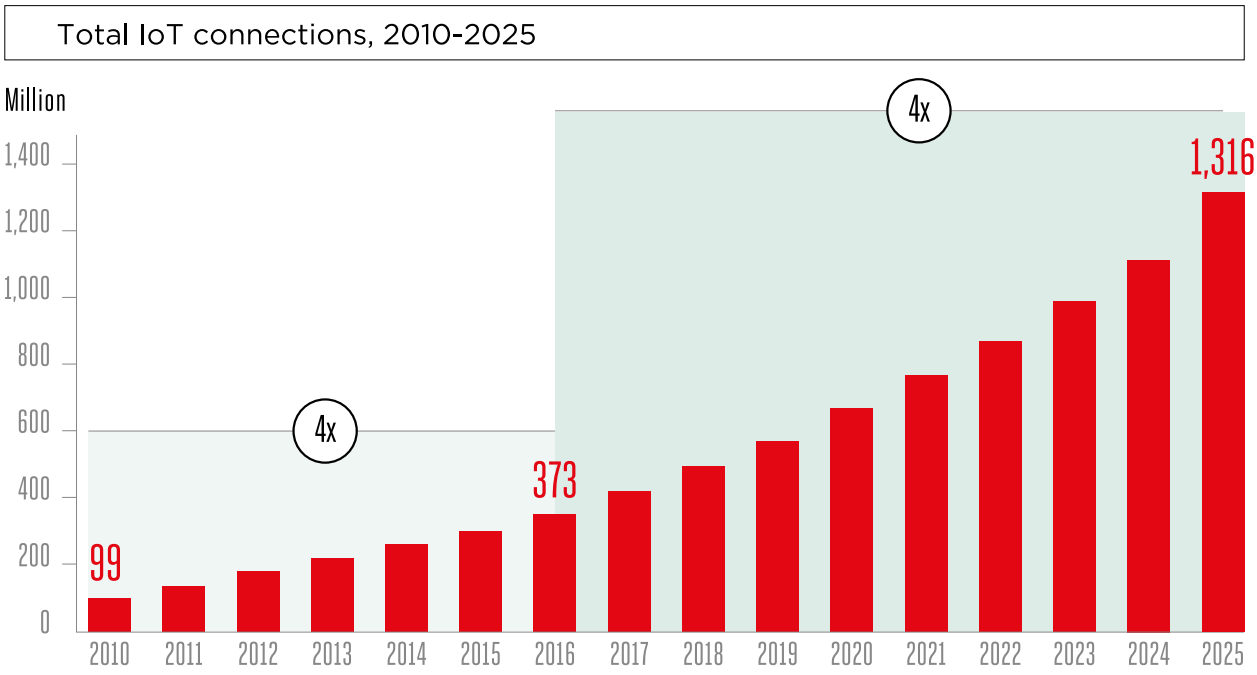
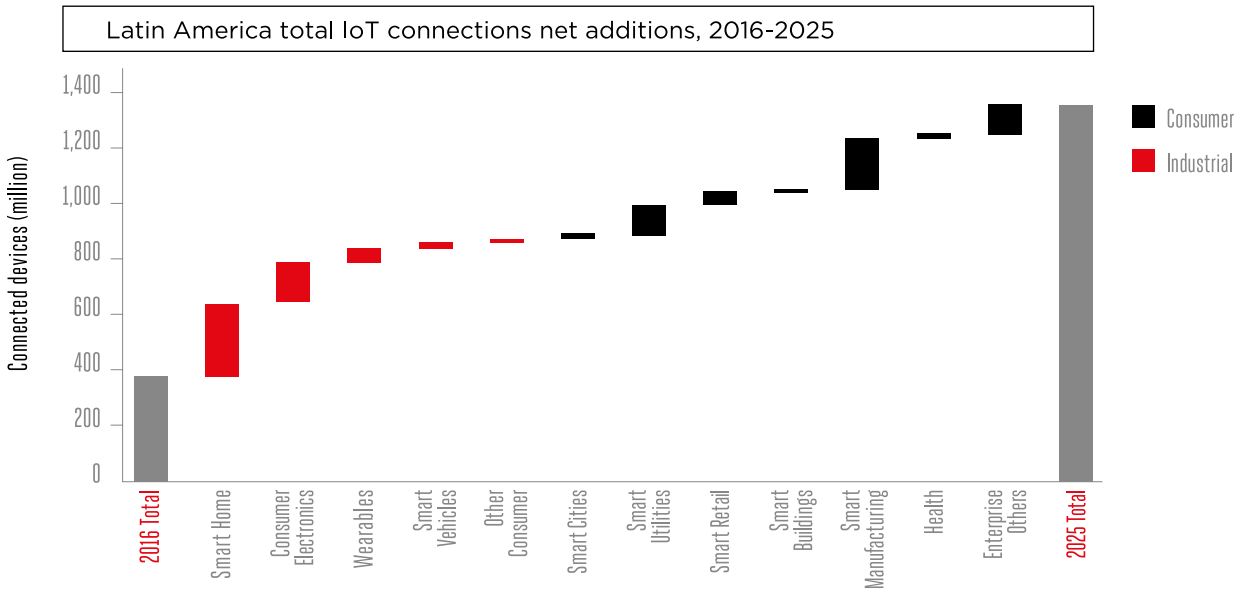


Figure 2: Total IoT Connections in Latin America, Net additions, 2016-2025
Source: GSMA Intelligence



Frontier Economics estimates that a 10 per cent rise in machine-to-machine (M2M) connections leads to annual increases of around 0.7 per cent in GDP and a 0.9 per cent increase in industry GVA.[2] The study is based on OECD data and covers a sample of OECD countries including Mexico and Chile. At the same time, A.T. Kearney predicts IoT will lead to a $1.9 trillion global productivity increase and $177 billion in reduced costs by 2020. It is important to highlight that the IoT will have an important impact on industries as well as for consumers, which will have the biggest expected growth in the region, particularly on smart home applications (see figure 2 below).

Here are some of the questions policymakers should start asking right now to set the right path for unleashing the potential of IoT[3] :

- What is the estimated impact IoT can bring in my country or municipality in 5 years?
- What are the key areas that can benefit the most from IoT (e.g. sustainable agriculture, manufacturing, water distribution systems, smart vehicles, healthcare, etc.)?
- How can policymakers (ministries, regulatory agencies, Congress, local governments) help create a sustainable IoT ecosystem that encourages innovation and local startups?
- What can be done to assure continuity of smart city projects throughout different administrations?
- How can small and medium enterprises (SMEs) benefit from a sustainable IoT ecosystem?

2. https://www.frontier-economics.com/media/1167/201803_the-economic-impact-of-iot_frontier.pdf
3. Refer to Annex 1 for a checklist of considerations and actions for building an IoT strategy.

2. CONSIDERATIONS IN MAKING POLICY FOR THE IOT

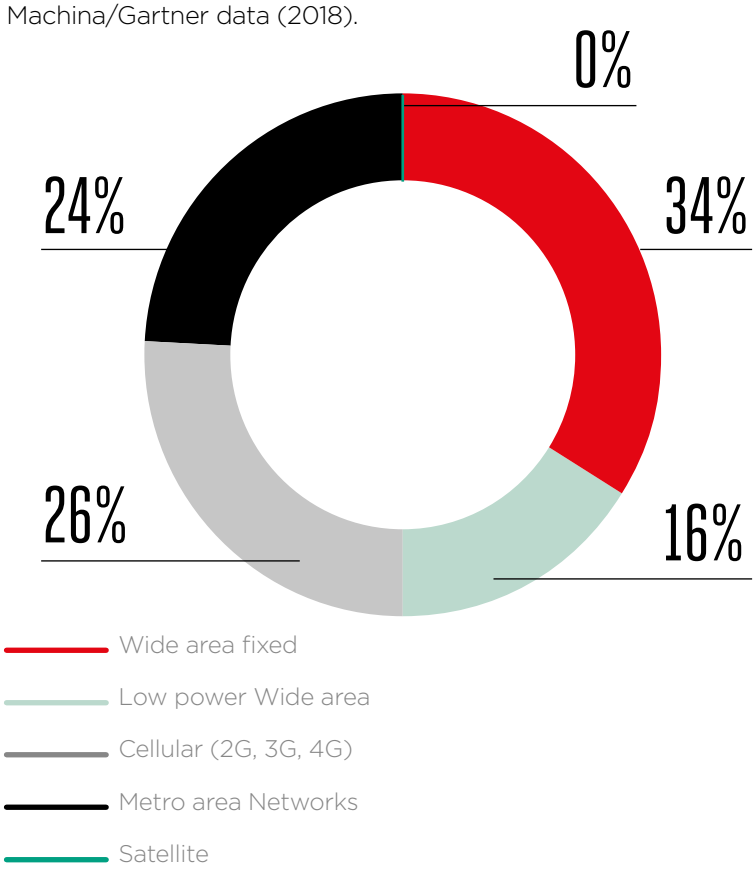
The Internet of Things describes the coordination of multiple machines, devices and appliances connected to the Internet through multiple networks. These devices include everyday objects, such as tablets and consumer electronics, and other machines, such as vehicles, monitors and sensors equipped with M2M communications that allow them to send and receive data.[4]
In practice, then, the IoT is not just about adding connectivity to "things", but, instead, using these things to capture and process data, thus supporting real-time decision-making and providing insights through big data and analytics. This creates important implications in terms of business models, competition, technology and policy-making.

2.1 BUSINESS MODELS AND COMPETITION IN THE IOT

The IoT ecosystem is both competitive and diverse: industrial players, vehicle manufacturers, technology firms, telecom operators, and new entrants and startups compete in one or more segments of the value chain.
There are some obvious differences between traditional voice and data services and IoT, such as the number of connected elements – likely to be substantially higher for IoT devices –, and the core service – not being centered in voice and data.

In the market for connectivity in the IoT, there is and there will continue exist a very healthy and dynamic infrastructure-based competition (see figure 3 below). Choice of connectivity will be driven by the intrinsic characteristic of the device, its mobility, its location, its bandwidth requirements and its complexity.
Out of the 1.2bn estimated connected devices in Latin America by 2023, only 306 million will be wide area. Of these, estimates that 79 million will be traditional mobile networks, 48 million Low power wide area (both licensed and unlicensed), 73.5 million will be Metropolitan area networks, and 100 million fixed connection, while only little over 1 million will be satellite.

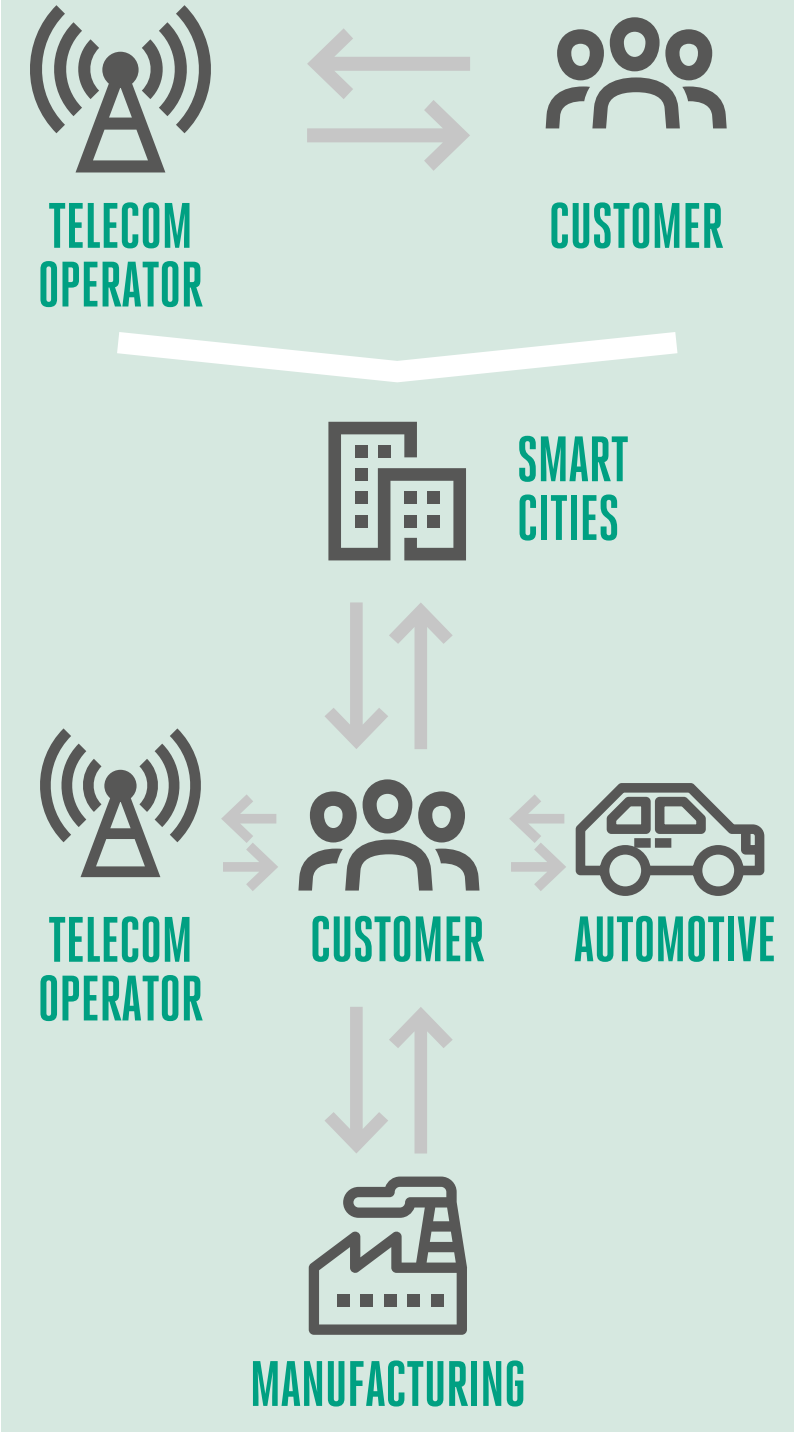
Figure 3: Wide area connections in Latin America by connectivity technology in 2023
Source: Own Elaboration on Machina/Gartner data (2018).



Connectivity enables data transfers and is a fundamental element of an IoT service, but is only one component of the product mix. The value generated by IoT services is essentially and intrinsically related to the data that sensors record and the analytics derived from them. This could be, for instance: data generated

4. This is a "definition" of IoT with which we can work – while it might seem useful at first to propose a stricter definition of IoT, the label "IoT" in fact encompasses a myriad of different products, services and solutions, and any rules based on a strict definition would likely not be applicable across the board.

FIGURE 4: DIFFERENCES IN BUSINESS MODELS BETWEEN TRADITIONAL TELECOMMUNICATIONS SERVICES AND IOT



by sensors to enable more efficient maintenance cycle and predictive analytics in industrial IoT; data on soil humidity, combined with weather informs better irrigation in smart agriculture; data about availability and location of vehicles with respect to potential users in the case of car-sharing to enable an innovative "product-sharing" business model.

Further, the average revenue per user (ARPU) is much smaller in IoT connections, as many IoT device rely on the exchange of very small amounts of data. A smart meter, for example, may share only few kilobytes every week or month with the back-end platform. This means that, when looking purely at the revenue from the communication networks, IoT most often tends to generate significant less traffic and revenues per device, as low as USD 2 per month, and even lower in some cases. Another key difference is how the ecosystem is built (see figure 4 below). While most communication providers sell directly to their own customers traditional voice and data plans; in the case of IoT, the relationship chain can be much more complex, beginning with the sale from suppliers to service providers, which in turn sell to the final customer (be it a consumer or another enterprise). The many particularities of the IoT explored above result in a variety of business models that can be developed, such as:

- Initial and ongoing fees, similar to more traditional models, where the initial fees reflect the cost of the device, and the ongoing fees are meant to cover the service charges;

- Ongoing fees, where no initial fee is charged and the costs are usage-based;

- Initial fee only, which consists of an upfront installation cost that also covers service fees;

- Savings-share, where an IoT solution is designed to reduce costs, and a share of the amount saved is paid to the service provider.

2.2 EXISTING POLICY BARRIERS TO THE IOT

Another important challenge regarding policymaking for the IoT is overcoming the existing policy barriers that affect the IoT in direct or indirect way, and lead to distortions in the market and damages to competition and innovation. Although discussing such barriers is not within the scope of this document, it is worth noting two important aspects: legacy regulation on connectivity and taxation.

One of the essential requirements to IoT is connectivity, which is intrinsically related to the country's telecommunications infrastructure. Heavy regulation of the telecommunications industry could effectively hamper the development of IoT, and an in-depth review of the laws and regulations governing the industry is necessary, including issues such as spectrum, numbering resources, type approval of devices, and other telecom-specific rules.[5] Ultimately, regulation should allow IoT services and their deployment to be relevant, fast, and innovative.

Further, taxes and fees applied on most services (not least of which connectivity) were created considering the economics of traditional services, and they often do not apply to IoT – in fact, charging high taxes can effectively prevent the massification of IoT and IoT-based solutions for the government, businesses and consumers. Due to the very low average revenue per user (ARPU), taxes and fees, on what concerns their application to IoT solutions, should be redesigned for minimal impact on price so as to not make many services economically unfeasible. To that end, decisionmakers can consider options such as full tax breaks or regulatory holidays.

5. For a review of best practices on IoT regulation refer to GSMA knowledgebase: https://www.gsma.com/iot/iot-knowledgebase

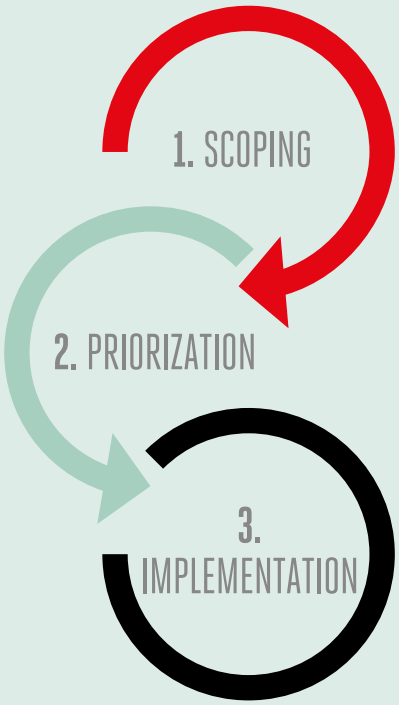
3. THE NATIONAL LEVEL: RECOMMENDATIONS FOR NATIONAL GOVERNMENTS

After understanding some key characteristics of the IoT that affect policy-making, it is easy to see why IoT can be a challenge for decision-makers in Congress, central government and national regulators. Around the world, many governments already have taken steps to support the growth of IoT. Governments in Latin America can assume the important role of building the ecosystem and being a major drive for demand. To that end, policymakers should carefully consider the three recommendations below.

3.1 DEFINE A LONG-TERM STRATEGY

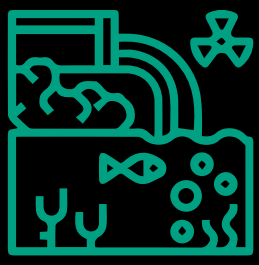
While differences between governance models from one country to another can be attributed to domestic context, the role of government in IoT should remain the same in every country: to stimulate building a strong IoT ecosystem. This, in turn, means to adopt actions to encourage innovation and reduce the risk of investing and innovating, including, but not limited to: direct investments, fiscal incentives, government contracts, supporting the building of clusters and accelerators, creating programs to support the building and adoption of IoT by small & medium enterprises (SMEs). To better understand exactly which actions to take and how to weigh their relevance, Latin American governments must first undergo a planning process consisting of three steps: scoping, prioritization and implementation (see Figure 5 below).

FIGURE 5: A 3-STEP PLAN FOR BUILDING AN IOT POLICY



Case of Brazil: planning an IoT policy

In a process that started in 2014 with the establishment of the then-called M2M Chamber (currently IoT Chamber), the Brazilian government created a permanent forum to regularly discuss, with the private sector as well as with other stakeholders at government, key challenges and priorities to make the growth of IoT possible in the country. This highlights the importance of involving the industry early on to have a better understanding of risk and opportunities, as well as to secure their buy-in from the start.



IoT and SDGs

The IoT can support the realization of the United Nations Sustainable Development Goals (SDGs) by 2030. Some IoT projects to support that goal would include reducing waste in water and electricity, monitoring of endangered species, and climate change mitigation.

SMART AGRICULTURE: IMPROVING FARM PRODUCTIVITY

According to the World Bank, the world will need to feed a projected 9.7 billion people by 2050, meaning an increase in food production of 50%. One way to increase the food output is to reduce food waste. The Food and Agriculture Organization (FAO) estimates that roughly one third of the food produced in the world for human consumption every year — approximately 1.3 billion tones — gets lost or wasted. In developing countries, 40% of losses occur at post-harvest and processing levels. According to IBM, 90% of all crop losses are weather-related, and predictive weather measurement through the application of precision agriculture systems, such as those enabled by IoT, can reduce this crop damage by about 25%.

Relatively simple solutions can help reducing waste increase the value to the farmer.

In 2018, Telefonica signed an agreement with FAO (United Nations Food and Agriculture Organization) to collaborate in the development of innovation, digitization and data analysis in the agricultural sector to promote the development of agriculture, food safety and nutrition, with pilot projects being developed in El Salvador and Colombia.

In developing markets, the agribusiness can derive enormous benefit from full and real-time visibility alongside the value chain. In Cordoba, Argentina, Claro built a partnership to develop an IoT solution for an agricultural exporter that connects machines and farm animals with sensors, and analysed drone and satellite images. The data consequently generated can be analysed through an online dashboard with reports, graphs, and predictive analytics. This gives traceability to products, and helps the producer meet the high standards of their international customers.

In the *scoping* phase, governments should seek to understand the national aspirations regarding IoT, as in what the country wants to and can realistically achieve within a set timeframe. It is important to involve as many stakeholders as possible in this stage via open-ended public consultations, and creation and participation in relevant forums and events. Brazil, for instance, has had a successful approach in creating the locus for exchange of views with the private sector as well as the wider ecosystem (including representatives from universities and civil society). At this stage, it is also useful to discuss the key values and long-term strategic objectives that will have to inform the government's actions, such as economic growth, improving productivity, improving and extending access to public service, improve response to natural disasters such as floods or deforestation.

In the *prioritisation* phase, governments should identify which verticals (e.g. agriculture, transportation, automotive, or energy) could produce the most benefits for the country when a full IoT ecosystem is enabled. Quantifying the effective economic benefits to the country should be on the basis of best practices and should open the path to evidence-based policy-making. On the other hand, identifying priority industries should not mean raising barriers for other industries, as that could slow down innovation and affect the overall benefits that can be brought by IoT. Proposed outcomes from the prioritization phase should undergo public consultation, and receiving inputs from the industry and the IoT ecosystem is essential in this phase. As a result of this process, the government should present a draft IoT policy and strategy which define specific actions and timelines, and KPIs (e.g. increased coverage of specific

services, cost reductions percentages, reduction of CO2, life saved etc.). However, governments should resist the temptation to 'choose for the market' specific technology solutions to roll out IoT services, as they may become obsolete very soon, or artificially tie a solution to a specific country or provider. It is important to let market and end-users choose. During the *implementation* phase, previously agreed actions should be monitored to measure goals. Both at central and local level, it is important to ensure that flexible legal avenues exist to enable managers to have the flexibility and independency necessary to innovate over the top. This may be achieved through the creation of a specific department for IoT, allocating dedicated budget, and creating incentive structures for the private sector to promote efficient investment of taxpayers' resources. Finally, all relevant government agencies must recognise the truly cross-department nature of IoT and the extremely dynamic technology evolution of these solutions, or else run the risk to define silos-based policy, failing to capture synergies with other sectors, increase cost to taxpayers, and ultimately fail to deliver. All relevant agencies (ministries, departments, and regulators) should therefore co-ordinate on long-term strategies, shared objectives, and work together to define policies, so as to avoid duplication of effort.

3.2 FOSTER DEMAND VIA GOVERNMENT PROCUREMENTS

The Internet of Things can have a positive impact in reducing the cost and increasing the agility of government services. Further, IoT can indeed have a key role in leapfrogging 20th century infrastructure challenges in Latin America (smarter utilities, building and maintaining roads and highways, allocation of security resources in crowded urban centers, etc.). As a part of a successful IoT strategy, governments in Latin America can play a key role in fostering demand for IoT, and therefore stimulating the creation of a strong IoT ecosystem. Therefore, governments need to identify key areas with significant deficiencies (such as public safety, urban mobility, or healthcare) and prioritise IoT solutions

IoT in a comprehensive digital agenda

In recognising the importance of the digital ecosystem and the move towards the digital convergence, government leadership in Latin America should aim to build a comprehensive digital agenda to support digital inclusion, a harmonized regulatory framework, new investments, infrastructure deployment, and the digitisation of production chains. Forward-looking policies in this regard will include IoT as one of its major components. Generally speaking, digital agendas, including IoT, should be in the platform of any political candidate running for a major office in Latin America.

to help overcome existing barriers. These solutions can be used either to optimise existing processes or to create innovative and cost-efficient solutions. Rules for government procurements, for instance, can prioritize IoT solutions, as long as they are cost-effective and/or are able to deliver more benefits than traditional solutions. As explained in section 2.1, the IoT allows for different business models, including savings-sharing, which can be a way for governments to award long-term contracts without incurring in any new costs. This can be, in fact, an opportunity for governments not to spend more in any critical area, but to be able to reduce costs and have a bigger bang for the buck. In addition, when designing rules for government procurements, policymakers should seek to avoid vendor lock-in and risk of no interoperability; to achieve that, governments only adopt scalable, future-proof and technologically-neutral solutions.

3.3 ADDRESS PRIVACY AND SECURITY

One of the key policy issues relating to the IoT that often requires positive action from policymakers is that of privacy. While data is global in nature, the regulation of data protection and privacy still remains a patchwork of non-interoperable provisions and requirements. Currently, there are more than 100 national and regional data protection frameworks, and sometimes even within a single country data protection is regulated by several different laws and regulations. Latin American policymakers should consider developing a privacy and data protection general framework, or, if they already have one, they should ensure that it is compatible with the IoT as well as the converging digital ecosystem and the move towards a data-based economy. This includes reviewing strict obligations on alternative requirements for processing data (such as explicit versus implied consent) and cross-border data transfers. When possible, decision-makers in the area of privacy and data protection should seek harmonization of rules, particularly on what concerns cross-border data flows, to enable innovation while ensuring a consistent level of protection for users. It important to note, however, that there is no need for an IoT-specific data privacy regulation. While many IoT solutions, such as those for farm and industrial uses, do not collect personal data and pose no threat for the privacy of users, where IoT will collect personal or personally identifiable data, consumers will be more consistently protected with a general-purpose data privacy framework, particularly if such framework is harmonised with international best practices in privacy and other national and regional frameworks.

Optimising gas supply in Ecuador

In Manta, Ecuador, Telefonica has developed an end-to-end solution for a company that offers integrated services for ship owners, ship operators, and other fishing and cargo-related companies. With GPRS-enabled sensors, the company is now able to monitor in real time their fleet operations, in particular monitoring and identifying gas consumption patterns, allowing them to optimise refilling schedules, identifying possible leakages, and ultimately reducing consumption. While based on data collection, this IoT solution brings no risk to individuals' privacy.

GSMA INDUSTRY SECURITY GUIDELINES AND SMART CITIES APPLICATIONS

IoT-based smart city applications raise the same types of cybersecurity issues as those contemplated in existing internet services, namely how to protect the availability, identity, privacy and integrity of the service components. One of the unique challenges of these services is how to achieve these properties in devices that most often are low complexity, low power, have long lifecycles and are physically accessible to attack.

One could imagine a smart 'connected' parking meter in a smart city that has to be developed at low cost, has to run on a solar powered power supply, has to be secure for ten years and is deployed on a public street which is accessible for 24 hours a day. It is easy to see that the security challenges of securely implementing such a product are non-trivial and that many physical and cyber security related challenges will need to be addressed.

The mobile telecommunications industry has a long history of providing secure products and services to their customers. To help ensure that the new IoT services, including smart city services, are coming to market are secure, the Network Operators (Carriers) together with their network, service and device equipment partners have produced a set of security guidelines to share their security expertise to service providers.

The GSMA guideline documents promote a methodology for developing secure IoT services to ensure security best practices are implemented throughout the life cycle of the service. The documents provide recommendations on how to mitigate common security threats and weaknesses within IoT services.

Source: GSMA Security Guidelines (https://www.gsma.com/iot/iot-security/iot-security-guidelines/)

On what concerns security and the IoT, it is important that governments support industry-led best practices and standards. With the IoT being a nascent industry, creating new standards for security (particularly if they are national rather than global standards) could harm innovation and, in many cases, not deliver the desired outcome (i.e. a more secure IoT device, service or application). As threats evolve, so do industry-led best practices and standards, which are quicker and more cost-effective to adapt than rigid national standards. This ensures the much-needed flexibility for the IoT ecosystem to adapt to new threats and scenarios. The role of government in this case can be, for example, to promote voluntary certification programs.

4. THE LOCAL LEVEL: MAKING SMART CITIES

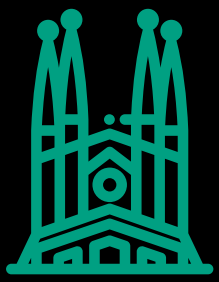
In Latin America, the most urbanised region in the world with over 80% of citizens living in urban areas, cities have an important role to play in the IoT ecosystem. Due to their size, geographical spread, entrepreneurial vibrancy and even infrastructure challenges, cities in the region can actively champion the deployment of IoT and enjoying the benefits brought about by the IoT. IoT and smart city applications can effectively pave the way for Latin American cities to leapfrog late 20th century challenges and become 21st century leaders, generating substantial socio-economic benefits for citizens and businesses. Policymakers should make the most of this opportunity, by designing and implementing smart city projects with an agile governance structure based on open and scalable systems, a positive and long-term vision that is defined around citizens' needs, and a culture of openness, innovation and transparency. Before setting out an agenda for a smart city, policymakers at the local level should consider the following recommendations.

4.1 PROMOTE COORDINATION AND CREATE A FLEXIBLE GOVERNANCE MODEL WITH AN INDEPENDENT LEADER

To build an effective smart city project, the city should start by: (i) appointing a service-oriented officer, such as a Chief Information Officer (CIO), empowered to develop and execute a strategic vision built to address citizen's needs; (ii) adopting an agile institutional framework and governance mechanisms; (iii) acknowledging that the it is not necessary to 'reinvent the wheel' at local level larger issues such as security and standards – stick to national/regional frameworks instead. Defining the right framework and governance for the projects to ensure flexibility and accountability is an important initial step.

Most smart cities projects require co-operation and information exchange between teams typically have not worked together before, such as divisions in charge of street lights and waste management, which would be adopting similar technologies. Co-operation is, therefore, fundamental, be it between city departments, local companies, and citizens. This is particularly true when using IoT sensors and Big Data to create a dashboard of the various services offered by the city; this, in turn, can be used to identify critical infrastructure issues and potential bottlenecks, which will help diagnose major problems in real time, such as security events, natural disasters and epidemics.

The project leader, typically referred to as CIO, will have the relevant authority to direct and oversee smart city projects across the municipal structure to avoid fragmentation or duplication of effort. To act efficiently, she will have the appropriate level of independence and will be targeted with strategic objectives such as resources or energy savings. A CIO will produce and implement a strategy capable of bringing along all agencies in a city, overcoming the lack of



BARCELONA:
a smart city coordinator

One of the most advanced smart cities in Europe, Barcelona has had a smart city coordinator for many years. Her objectives are to oversee smart city initiatives and coordinate them across departments and, most importantly, to define a long-term strategic vision for the city.

SINGAPORE:
CIO AND GOVTECH

One of the most advanced smart cities in the world, Singapore has given its CIO responsibility for the GovTech agency formed to oversee innovation for the Smart Nation strategy. The CIO is leading a number of advanced smart city projects including Virtual Singapore, and Beeline, an app for citizens without easy access to public services, that crowdsources bus routes.

co-operation, the fear in exchanging data, the insufficient funding and ultimately the cultural resistance in the city's departments. Rather than a focus on the technology or the solution, the CIO needs to understand citizens' needs, build an understanding of the various options and the long-term strategy, and be able to effectively communicate the benefits.

4.2 DEVELOP PARTNERSHIPS AND SEEK DIVERSE FUNDING & INVESTMENT OPTIONS

One of the most recognised barriers to smart city deployments in Latin America is the lack of resources within the local government. The perception of a resource-constrained local administration has understandably led many city officials to close the door for potentially innovative projects in their respective jurisdictions. However, as explained in section 2.1, one of the novel aspects of the IoT is its diversity of business models. When compared to many traditional offerings of public services, IoT solutions can offer new opportunities for local governments with a business model based on savings-share, for instance, which would have no upfront costs for the local government.

After having completed a cost-benefit analysis on the smart alternatives for delivering traditional public services – from utilities to traffic management –, local governments should seek partnerships with the IoT ecosystem to deploy cost-effective, technologically neutral, and scalable solutions. In addition to straightforward government procurement, local authorities can seek to develop different models of public-private partnerships (PPPs). In authorizing the private sector to take responsibility for delivering a public service, local governments can define the principles for the offering of the service (such as quality, interoperability, and scalability) and monitor their implementation. This not only reduces the operational risks of having the government deploy such infrastructure and services, but also can help ensure the cost-effectiveness of the solution.

SMART LIGHTING IN BRAZIL AND COLOMBIA

Caraguatuba is a coastal town in the state of São Paulo with more than 110 thousand inhabitants. In 2017, it became one of the first cities in Brazil to develop a PPP for public lighting. The project has the goal of changing 100% or 18,000 of the city's street lamps for smart LEDs that can feed into a dashboard that can be monitored by the local government. The new light poles in Caraguatatuba can also be used in the future for other smart city applications.

In Colombia, Claro is working with a municipality to pilot a smart lighting project that will allow street lights to dimmer themselves according to time of day, season, and presence of pedestrians. They will also be able to send maintenance alerts and preempt possible failures.

4.3 ADOPT OPEN, SCALABLE TECHNOLOGIES AND FUTURE-PROOF SYSTEMS

Cities contain hundreds of systems and services. Not all services have to become smart, but having them linked by a common infrastructure and standards-based technologies is an essential foundation based upon which the long-term evolution of a smart city can be built. As the deployed technology will need to last decades, it must be cost-effective and flexible enough to grow (scalability) and to support many changes and new services in the future (future-proof). When an IoT service is scalable, it means the technology solution can be adopted to adjacent services relatively seamlessly and with reduced deployment costs so to maximise economies of scale and scope that the initial investment can generate. Mobile technology solutions, particularly such as those illustrated in the box below are by definition scalable, as they capitalise on an existing coverage already provided for voice and data services therefore the marginal costs of adding additional IoT solutions that use the same networks will be limited. To be future-proof, an IoT solution means that the technology choice is robust enough to withstand the future evolutions and avoid the risk that the solution will become obsolete very quickly, and thus increasing maintenance costs and tying in the administration to a single supplier. Mobile IoT technologies will offer the advantage of utilising a wide variety of suppliers and relying on global technology specifications defined by industry standardisation bodies, which are regularly updated to meet new use cases and are tested worldwide. Finally, it worth noting that many components of a smart city solution (e.g. communication networks, cybersecurity, data analytics tools, etc.) can be applied and shared across a multitude of different services: from smart metering to traffic management, smart street-lights. Sharing components in this way should reduce set up and maintenance costs.

SMART CITIES AND MOBILE: MOBILE NETWORKS FOR IOT

Mobile operators can be knowledgeable partners to Latin American cities. They can enable secure, scalable and robust smart city solutions. As well as being well placed to understand both local city dynamics and international best practices, mobile operators typically have a commercial presence in the city and run advanced and secure networks that can scale easily.
Mobile IoT connectivity can enable simple on/off type applications, such as street lamp controls, air quality monitoring, parking sensors and basic status updates for many types of sensors, including those that are battery powered and located in inaccessible places for years.
The key advantages of Mobile IoT technologies are very low power consumption (with battery duration in excess of 10 years for some applications), very low modules costs, good indoor and extended outdoor coverage, plus the typical benefits of mobile networks: easy scalability, high level of security, easy maintenance and integration into unified IoT platforms.
The mobile industry is now deploying networks specifically designed to support the Internet of Things (IoT).

4.4 OPEN DATA: MAKE SELECTED CITY DATA AVAILABLE TO THIRD PARTIES THROUGH PORTALS TO PROMOTE TRANSPARENCY AND STIMULATE INNOVATION

Cities generate a wealth of data sets encompassing transport, the environment, health, demographics, services accessibility and other areas. Whether used by policy-makers, researchers, media, entrepreneurs, city event planners, or application developers, city data is an increasingly valuable asset that city managers must capitalise on. While protecting privacy and maintaining public trust, city officials should make these valuable data accessible so that it can easily be used by citizens and commercial entities to create innovative services.

As well as providing one-stop access to a city's information, sharing data helps communication and analysis, more transparent and efficient policymaking, and, most importantly, creates value by catalyzing the development of innovative apps and services.

This practice, which is already adopted by many cities throughout the world, can help enable a vibrant big data ecosystem in the city.

OPEN DATA IN SMART CITIES

London: The Greater London Authority makes available 705 data sets on its London data store.

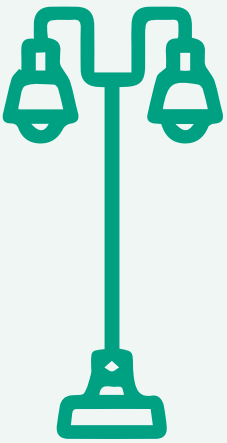
Copenhagen: The city data exchange provides a service for the sale, purchase and sharing of a wide variety of data from multiple sources between all types of users in a city – citizens, city government and businesses.

Singapore: A central government initiative, 'Data.gov.sg.', was launched in 2011 as a one-stop portal for publicly-available datasets from 70 government agencies. More than 100 apps have been created using this data.

Melbourne: The city of Melbourne has built a portal to make data available on a non-commercial basis. Melbourne is making available a growing catalogue of data sets grouped under assets and by category, such as infrastructure, economy and environment.

ONE PLATFORM, MANY SERVICES

Smart lighting application have the potential to go beyond energy savings. Light posts can also be used as platform for other services. Since launching its Smart Cities organization in 2015, AT&T has been using its resources and IoT expertise to create impactful solutions for cities. By introducing GE's Predix-powered IoT platform, AT&T can use outdoor LED lighting in a city to create a digital infrastructure that helps address issues like traffic flow and parking optimization, gunshot detection on city streets, air quality monitoring and weather emergency alerts. They have recently announced a deal with the City of San Diego to upgrade thousands of the city's outdoor light fixtures to sensor-enabled LED technology, making it the world's largest smart city IoT platform. AT&T will act as the data carrier and provide highly secure connectivity for the San Diego deployment, which is expected to save the city approximately $2.4 million in annual energy costs.



Annex 1

Checklist of actions for IoT policymakers

TOPIC	QUESTIONS	YES	NO
1. Perform scoping exercise	Are there clear and objective goals (for example, improving productivity, reducing congestion, reducing carbon footprint, reducing cost of delivery of public services, improve road safety, among others) with fostering IoT in the country or municipality? Are these objectives framed as deliverables (such as a percentage decrease in cost for a given service) without defining a specific technical solution or standard?		
	Are national or local circumstances (for example, current level of economic growth, economic dynamism, connectivity infrastructure, legal and regulatory barriers, capacity for investment, etc.) taken into account in the scoping exercise? Has a cost-benefit analysis been used		
	Are all relevant stakeholders – relevant ministries and regulatory agencies, development banks, mobile operators, device and equipment manufacturers, industry associations, among others – involved in this task?		
2. Prioritize areas of work[6]	2.1 Have decisionmakers considered and/or identified the key industries, sectors, geographies and/or services where the application of IoT could deliver the most value? What are they?		
	What is the size of this impact (which can be expressed in local currency or as a percentage of GDP) in the short (up to 1 year), medium (up to 5 years) and long run (5+ years)?		
3. Consider the privacy and security frameworks[7]	3.1 Does the country have a general data protection law? If so, have decisionmakers assessed the impact of such framework on IoT services (including in understanding where the data collected by a device or service is personal data)? In the case of municipalities, have they resisted the temptation to create local and specific consumer protections rules?		
	3.2 Is the privacy framework based on internationally recognized principles and light-touch on issues such as explicit consent (for example, not requiring a new consent for at every step of processing of data)?		
	3.3 Does the country have a cyber security framework? If so, it is based on industry best practices?[8]		
4. Foster demand	4.1 Are there safeguards against vendor lock-in?		
	4.2 Are solutions based on international standards and best practices?[9] Alternatively, have decisionmakers avoided imposing nationally defined technologies and standards?		
	4.3 Are solutions scalable and interoperable with other solutions and providers? For instance, if tomorrow decisionmakers wish to add additional services and/or coverage, would this be easily achieved at relatively low costs? Similarly, are services capable of seamlessly integrating existing and possible future services?		
5. Seek (and/or offer) diverse funding options	5.1 Have decisionmakers considered different instruments to promote investment in IoT, such as tax rebates, interest-free loans, lines of credit, specific measures for depressed areas, and public-private partnerships?		
	5.2 Have decisionmakers sought partnership with national, regional or international development banks?		
	5.3 Is there a long payback period for IoT-related lines of credit?		
	5.4 Have investment-friendly Public-Private Partnerships been considered?		
	5.5 Have stakeholders considered innovative business models such as those based on savings-share?		
6. Identify the right institutional framework	6.1 Has the IoT service been launched through an initiative undertaking whose decision-making process is sufficiently independent and flexible from traditional public administration departments? In other words, are decisionmakers able to react in a timely manner to project needs and possible changes?		
	6.2 Are decisionmakers able to handle procurements, consultants and finance independently?		
	6.3 Are decisionmakers able to facilitate cross-department communication with other government agencies, departments or offices (such as the Ministry of Communications coordinating efforts with the Ministry of Transport and the transit regulatory authority)?		
7. Appoint an officer to act as Chief Information Officer (CIO) with a strategic vision	7.1 Is it clear for decisionmakers in a municipality that the focus of the officer and its plan should be on services and citizen needs, NOT in specific technology solutions? Similarly, does the officer understand city and citizens' needs and how they are likely to evolve? Is the officer capable of understanding technology options without focusing on the technology solution?		
	7.2 Does the officer have a long-term strategy to roll out services? Accordingly, will the officer remain in this position long enough (at least 3 to 5 years) to allow for an IoT strategy to be fully implemented from scratch? Further, is the officer able to act independently, yet remaining accountable to concrete objectives (e.g. amount of energy savings in a year)?		

6. Refer to Annex 2, which contains principles on how to measure this economic impact.

7. It is important that policymakers resist the temptation of creating specific privacy and security rules for IoT; the best way to approach it is to support applicable international standards and utilize horizontal rules that apply consistently for all industries, thus fostering a more reliably protected and interoperable ecosystem.

Annex 2

Principles and premises for quantifying IoT and its economic impact in a country

Correctly identifying and quantifying the IoT phenomenon is a first step to establish well-defined, evidence-based policies focusing on the correct targets. However, the definition of IoT and its economic impact are still at an evolving stage. Therefore, the GSMA understands there is a need to try and homologate and standardise these definitions internationally so that national institutes of statistics can make meaningful comparisons and quantify the impact of IoT in their countries.

Some suggestions, in the form of principles and premises, are offered below to support the analyses and studies of the economic impact of IoT in a country or economic sector.

CONNECTIONS

ITEM	RECOMMENDATION
Definition of IoT	Defining what is an IoT device can be a complex task. It is a relatively new industry and many sources offer different definitions. Typically, an IoT service will combine four main basic elements: (i) Network/Connectivity, (ii) Data, (iii) Sensors/Actuators, and (iv) Device. Network connectivity is the fundamental enabler of an IoT device and is generally provided via Internet or at least IP protocol, but it closed networks can also be used. Connectivity is often not used to provide generalized access to internet or any-to-any traditional voice services. Data is another fundamental element. It usually comes from multiple sources (e.g. a connected thermostat combining humidity, movement sensors, with weather forecasts), but could also be one single source: a smart meter measuring gas consumption. Sensors can be one-way or actuators (i.e. two-ways communication), enabling the device to react to a specific condition (e.g. refill tank when level is low). Finally, the 'device' element is where sensors are embedded. This can be achieved by retrofitting an "old" through aftermarket solution (e.g. a car or a tractor) or by designing a new device entirely (e.g. a smart glucose meter reader), whose functionality is enabled by innovative connectivity. For statistics and forecasts, the GSMA intelligence defines IoT as: *"Devices capable of two-way data transmission (excluding passive sensors and RFID tags). It includes connections using multiple communication methods such as cellular, short range and others. It excludes PCs, laptops, tablets, e-readers, data terminals and smartphones."*
IoT services vs. other services	The above definition importantly distinguishes between IoT and other traditional voice and data connections excluding tablets smartphones and similar. A general guidance can be to identify the primary use of the service/device. An IoT service should be characterized by a service use which is not primarily voice communications and generalized access to internet. This does not mean that the IoT service cannot have such functionalities, only that they are rarely the focus of the service (e.g. an in-car emergency call service will establish an automatic voice connection to emergency services in case of an accident, but it cannot be used to make calls on a regular basis).
IoT devices vs. sensors vs. connections	The same object or device may have multiple services, based on independent sensors, which in turn have their own connections. E.g. a car (connected device) may have multiple sensors which make use of wide area networks and/or multiple SIMs. Comparing different analyst figures can therefore be confusing depending what they measures: one car, many embedded sensors connecting with the outer world, the type of connectivity that they use. There is no right or wrong here, but it is important to be consistent particularly when comparing data from different sources and countries. Given the focus on the connectivity market, GSMA Intelligence measures the number of connections. (see definition above)
Local vs. Wide area connectivity	One single device may combine local and wide area network connections. For example, a smart home device will connect indoor short/range through Wi-Fi, Bluetooth or ZigBee and will also use a fixed or mobile broadband for wide area network connectivity. Many other possible connectivity architectures are possible. For example, some devices only use LPWA, Satellite or fixed networks. The vast majority of devices will have at least a short range connectivity element and "concentrate" to a gateway. It is nonetheless important to distinguish between short range and wide area and monitor connectivity markets separately and independently.
Wide area alternatives	Appropriate wide are connectivity solutions make the difference for IoT. On top of fixed, satellite and mobile networks, it is important to count Low power wide area connectivity. These can be Licensed (on cellular network: technologies such as NB-IOT or LTE- M) or unlicensed solutions. LPWA licensed and unlicensed are expected to be the fastest growing connections for IoT.
Consumer vs Industrial	It should be considered aggregating the various verticals of IoT in two main categories – Consumer vs. Industrial, to simplify the analysis and comparisons.
M2M vs IOT connections	M2M and IoT definitions are often used a synonymous. GSMA defines Machine-to-Machine connections as: *"A unique SIM card registered on the mobile network (...) enabling mobile data transmission between two or more machines. It excludes computing devices in consumer electronics such as e-readers, smartphones, dongles and tablets.* Comparing the definition with the one provided above for IOT one can identify the key differences being: (i) M2M is provided on Wide Area Cellular network (ii) M2M is a point-to-point connectivity between machines only whereas IoT can include multiple sensors being connected through a short range connection. For example in car, multiple sensors can be connected short range (or wired) to a single point gateway. The gateways' module contains a SIM enabling the wide area M2M cellular connectivity.

REVENUES AND ECONOMIC IMPACT

TOPIC	RECOMMENDATION
Total IoT revenue vs. Connectivity revenue	The IoT is characterized by a long value chain and total revenues generated by the IoT industry include the application, device, and 'service wrap', as well as services such as 'data monetization' and service integration. IoT connectivity is a fundamental enabler but likely attracting a relatively small share of the revenue associated with the total IoT industry. A good estimate is 2% to 5% depending on Analysts house and data aggregation. The key point for policy makers is that policy enabling IoT do have a far wider outreach on the economy than just connectivity revenue. It is important that economic and statistics institute separately quantify the IoT total industry revenues and IoT connectivity revenues.
IoT Revenues vs Wider socio economic benefits	IoT has the potential to produce significant socio economic benefits to society, such as increasing productivity, reducing road traffic congestion, reducing carbon footprint, reducing PA spending in the provision of essential public services such as healthcare, reducing energy consumption. Well defined, evidence-based policies will set quantifiable objectives in each one of these dimensions. . It is therefore important that governments statistics office make an effort to define and quantify the economic impact of IoT so that it can be used for comparison with international peers and to set policy goals.

Annex 3

Existing IoT Standards by vertical

CELLULAR TECHNOLOGIES	VERTICAL	APPLICATIONS	CONNECTIVITY DRIVER	PERFORMANCE (INDICATIVE)
NB-IoT, LTE-M	Smart cities	Smart lighting, Waste management, Smart parking, smart bikes, smart utilities	Low power consumption, wide area coverage	• Up to 10 years battery life[10]; • Increased coverage compared to LTE (up to many times the radius of a standard cell depending on operational conditions)
	Smart agriculture	Water quality, live-stock monitoring, pest control	Outdoor/ Rural area coverage, low cost, service continuity	• Low power and Increased coverage (as above) • Ease of deployment • Low cost – modules prices to drop fast to 7USD in 2025[11]
Cellular V2X (network and direct mode)	Automotive	Vehicle-to-everything(V2X), mapping, software updates, infotainment, telemetry;	Ultra-low latency (safety related apps), ubiquitous coverage, wide installed base	• C-V2X offers over450 mt[12] in direct mode, wide area coverage in network mode; • Up to 90% vehicles with embedded cellular modems by 2025.
LTE	Drones	UAV Traffic management, ID registration, geo-location	Aerial coverage,	• Up to 400ft above ground level[13] vertical aerial coverage

8. Refer to GSMA IoT Security Guidelines.

9. Refer to Annex 3, which lists existing standardization bodies for IoT.

10. 3GPP- TR 45820 https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2719

11. https://www.gsmaintelligence.com/research/2018/07/spurring-adoption-of-nb-iot-notes-from-china/685/

12. https://www.qualcomm.com/media/documents/files/accelerating-c-v2x-commercialization.pdf

13. https://www.qualcomm.com/news/onq/2017/05/03/qualcomm-technologies-releases-lte-drone-trial-results

Annex 4
Existing IoT standardization bodies

Given the wide nature of the industry, a wide variety of standardisation bodies already exist that are related to IoT. This section is focused on the ones most relevant from a connectivity and service layer perspective.

3GPP

The third generation partnership project (3GPP) is the industry technical specification body. Representatives from all the seven main standard development organizations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC) participate to 3GPP. 3GPP produces technical specifications for connectivity communications which in turn are encapsulated in standards defined by standard development organizations. 3GPP covers cellular telecommunications network technologies, including radio access, the core transport network, and service capabilities - including work on codecs, security, quality of service - and thus provides complete system specifications. The specifications also provide hooks for non-radio access to the core network, and for interworking with Wi-Fi networks. Specifically on IoT, 3GPP has recently produced technical specification for radio access technologies for Narrowband IoT (NB-IoT) and Long term evolution machine type communication (LTE-M) with Release 13 (2016). The key advantages of these specifications in the context of IoT are:

- Low power consumption that enables devices to operate for 10 years on a single charge
- Low device unit cost
- Improved outdoor and indoor penetration coverage compared with existing wide area technologies
- Secure connectivity and strong authentication
- Optimised data transfer (supports small, intermittent blocks of data)
- Simplified network topology and deployment
- Integrated into a unified/horizontal Internet of Things (IoT)/ Machine-to-Machine (M2M) platform, where operators have this in place
- Network scalability for capacity upgrades

ONE M2M

The purpose and goal of oneM2M is to develop technical specifications which address the need for a common M2M Service Layer that can be readily embedded within various hardware and software, and relied upon to connect the myriad of devices in the field with M2M application servers worldwide. oneM2M prepares, approves and maintains the necessary set of Technical Specifications and Technical Reports for:

- Use cases and requirements for a common set of Service Layer capabilities;
- Service Layer aspects with high level and detailed service architecture, in light of an access independent view of end-to-end services;
  - » Protocols/APIs/standard objects based on this architecture (open interfaces & protocols);
  - » Security and privacy aspects (authentication, encryption, integrity verification);
  - » Reachability and discovery of applications;
  - » Interoperability, including test and conformance specifications;
  - » Collection of data for charging records (to be used for billing and statistical purposes);
  - » Identification and naming of devices and applications;
  - » Information models and data management (including store and subscribe/notify functionality);
  - » Management aspects (including remote management of entities); and
  - » Common use cases, terminal/module aspects, including Service Layer interfaces/APIs between Application and Service Layers, and Service Layer and communication functions.

ETSI

ETSI is the recognized regional standards body in Europe – European Standards Organization (ESO) – dealing with telecommunications, broadcasting and other electronic communications networks and services. ETSI is involved in standardising many of the technologies used to connect 'things' in the IoT.

- M2M
  - » ETSI is a member of oneM2M, the global partnership initiative which aims to provide a standardized M2M interface. This will enable different devices to be connected in the IoT, irrespective of the underlying network. The work of oneM2M builds on the activities of the ETSI committee TC SmartM2M, which has developed, and now maintains, the ETSI specifications for a standardized platform:
  - » Requirements (ETSI TS 102 689)
  - » Functional architecture (ETSI TS 102 690)

INTERFACE DESCRIPTIONS (ETSI TS 102 921)

- **IoT applications**
  Smart appliances
  Smart metering
  Smart cities
  Smart grids
  eHealth
  Intelligent Transport Systems
  Wireless Industrial Automation

- **Other IoT-related aspects**
  Security for the IoT
  Low power supplies in the IoT
  Radio spectrum requirements
  Embedded communications modules
  Multi-access Edge Computing
  Information Management
  Smart Card Platform
  Network Virtualisation

IEEE IOT INITIATIVE

The Institute of Electrical and Electronics Engineers (IEEE) also has a role in the standardization of IoT, known as the IEEE IoT Initiative.
The mission of the IEEE IoT Initiative is to serve as the gathering place for the global technical community working on the Internet of Things; to provide the platform where professionals learn, share knowledge, and collaborate on this sweeping convergence of technologies, markets, applications, and the Internet, and together change the world.
The IEEE IoT Initiative has worked on a number of issues, including standards for ethernet, coexistence of Wireless Personal Area Networks with other wireless devices operating in unlicensed frequency bands, mesh topology, smart grid, e-health and others.

INTERNET ENGINEERING TASK FORCE (IETF)

IETF is an open international community of network designers, operators, vendors, and researchers developing internet standards for the evolution of the Internet architecture. Several IETF working groups, are developing protocols that are directly relevant to the IoT, i.e. CoAP, TLS/DTLS.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO)

ISO is an international organization based on membership of national standards bodies, like ABNT in Brazil.
The most popular standards produced by ISO is ISO 9001 for Quality Management, ISO 8601 Date and time format, ISO 3166 Country codes, ISO 50001 Energy management, with a variety of sector specific standards.

GSMA

The GSMA represents the interests of mobile operators worldwide, uniting operators with companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. GSMA is providing a wide range of specifications and principles related to the interoperability among mobile operator. Other noteworthy areas of work include the IMEI allocation and database, roaming, billing, testing, security, etc.

GSMALA.COM