

With the Internet of Things (IoT) everywhere, can regulation be far behind?

How ICT regulators can enable IoT ecosystem development

Content

Executive summary	3
1.The increasing prominence of the IoT	4
2.The challenge for ICT regulators	5
3.Where the big debates are	6
4. Sharing of public IoT infrastructure: The more the better	9
5. How ICT regulators can lead with holistic frameworks	10
Conclusion	11

Authors:



Rajesh Duneja

Principal, Telecommunication,
Information, Media & Electronics, Dubai
duneja.rajesh@adlittle.com



Hariprasad Pichai

Principal, Telecommunication,
Information, Media & Electronics, Dubai
pichai.hariprasad@adlittle.com



Andrea Faggiano

Partner, Telecommunication,
Information, Media & Electronics, Dubai
faggiano.andrea@adlittle.com



Thomas Kuruvilla

Managing Partner, Telecommunication,
Information, Media & Electronics, Dubai
kuruvilla.thomas@adlittle.com

Executive summary

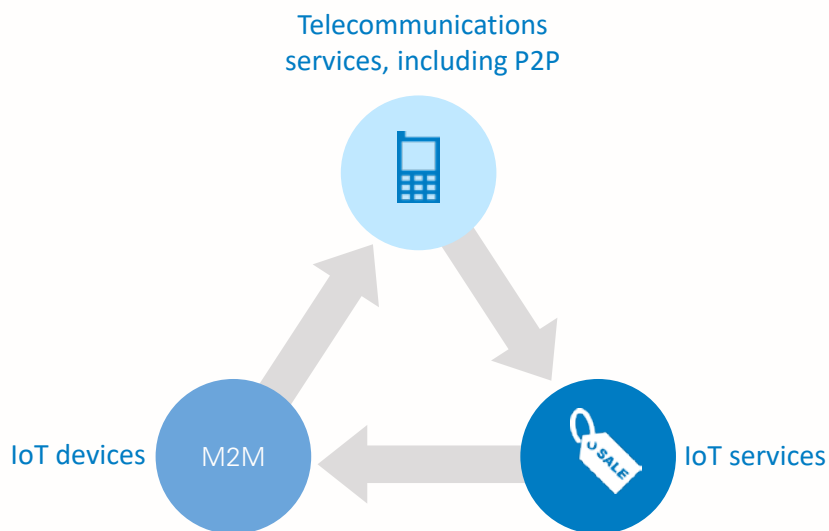
The IoT ecosystem is expected to grow rapidly in the next few years, with mainstream deployment already prevalent across many vertical industries. Increased IoT penetration across use cases poses unique challenges for ICT policy-makers and regulators beyond traditional telecom-focused regulatory topics such as spectrum, numbering, and roaming. The complexity and scale of the IoT brings increased focus on elements such as the safety of various stakeholders, new business models, data security and privacy. Given the potential benefits of the IoT, growth can be accelerated, and some of the pitfalls are avoided at the same time by effectively involving other national departments and ministries in addition to telecom regulators.

1. The increasing prominence of the IoT

Telecom operators and regulators have historically focused on person-to-person (P2P) telecommunications services. But the IoT ecosystem involves interaction of telecommunications services with a range of new services and M2M communications. (See Figure 1). The IoT will enter into every aspect of our lives and our cities, as well as support all industries.

ICT service providers and leaders in their respective industries are accelerating their efforts to tap this potential.

Figure 1: The Internet of Everything and Everyone








Source: Arthur D. Little

2. The challenge for ICT regulators

IoT use cases blur traditional industry-specific boundaries (see Figure 2) and challenge governance of industry verticals by respective sector authorities (see Figure 3). In addition, success of the IoT is dependent on collection and use of data to provide customized solutions, which poses a significant threat to consumers' data privacy and security. So there is an emerging trend to develop regulations which are case specific, as we have seen in the cases of drones and consumer data privacy protection. But these regulations are being developed independently. So far only New York State has issued a comprehensive IoT policy, which not only covers data privacy and security, but also plans to make information about IoT infrastructure public and share IoT infrastructure through public-private partnerships.

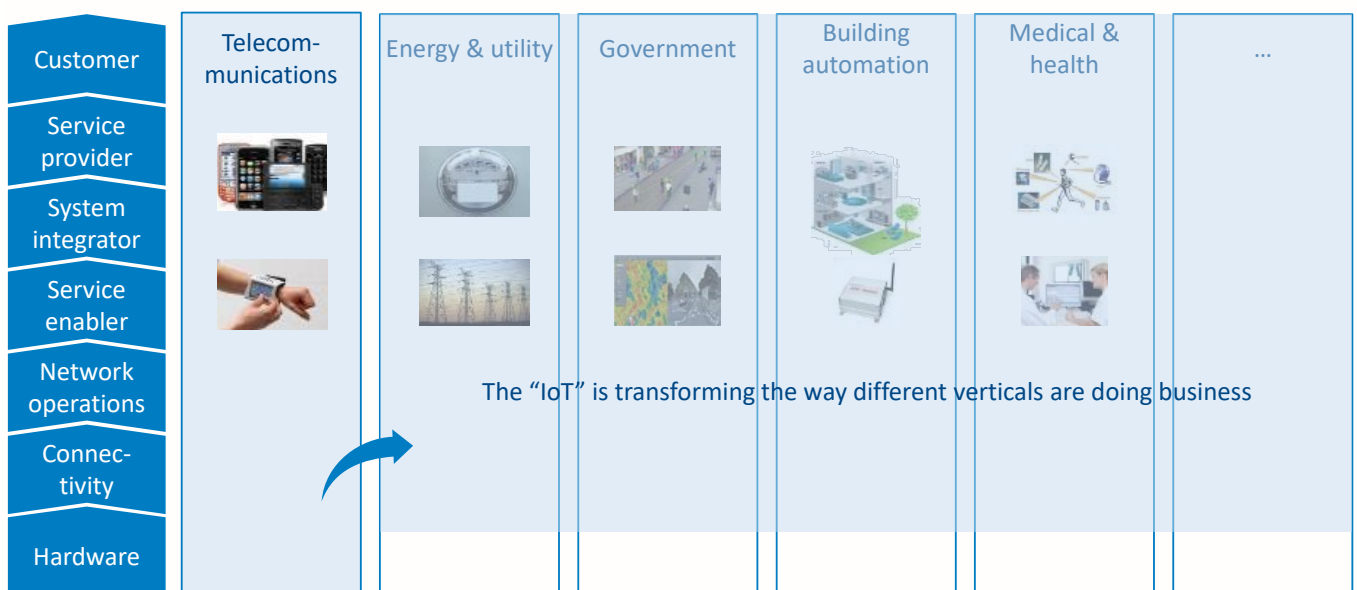
Accordingly, investors into the IoT ecosystem seek clarity on what is regulated or unregulated and permitted or prohibited. This situation makes it even more critical that policy-makers have holistic views for better management of the IoT ecosystem. ICT regulators are better placed to coordinate this cross-sector effort. In this document, we examine the regulatory challenges in developing a successful IoT ecosystem.

Figure 3: Vertical overlap in use cases

	Autonomous cars	Transportation?	ICT?
	Smart metering	Utilities?	ICT?
	Mobile payments	Financial services?	ICT?
	Remote health monitoring	Healthcare?	ICT?
	Flood sensors	Environmental?	ICT?
<i>...and many more!</i>			

Source: Arthur D. Little

Figure 2: Enhanced role for ICT service providers



Source: Arthur D. Little analysis

ICT service providers' play

3. Where the big debates are

We highlight the main debates across the following six traditional and upcoming areas that are being examined by regulators:

1. Licensing & spectrum
2. Switching & roaming
3. Addressing & numbering
4. Competition
5. Privacy & security
6. Sharing of public IoT infrastructure

1. Licensing & spectrum: More devices, more bandwidth!

Traditionally, many telecom regulators have been involved with type approval of telecom equipment. However, with the proliferation of IoT capabilities embedded into a diverse range of devices, this process will be inadequate. As IoT devices are evolving, connected things get a level of autonomy that has legal implications (e.g., connected cars). IoT regulation will have to define the responsibility chain and ensure IoT devices can be traced back to legally responsible persons and entities. This will entail regulators requiring registration to ensure fixing responsibility. Recent regulations about drone registration are an example of the evolving nature of IoT regulation.

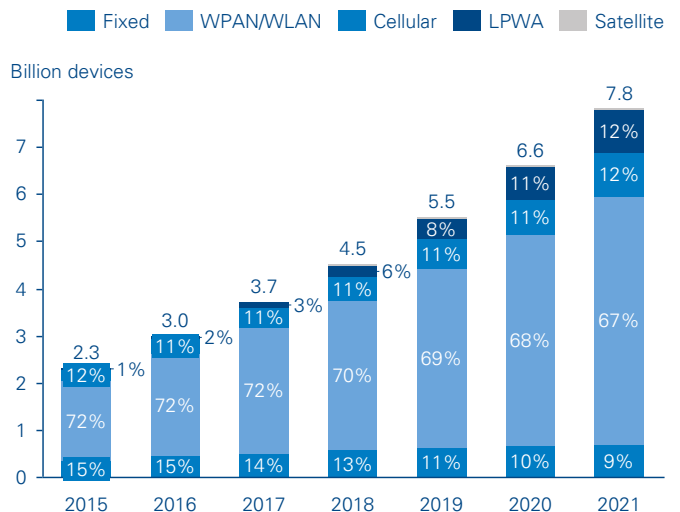
The situation becomes even more complex when many devices may be used in “mission-critical” cases in which their failure may affect a large number of people or lead to physical harm to an individual.

Given the complex and varied functionality of devices, telecom operators may not have the adequate expertise to type approve the devices. For example, as the Internet of Medical Things (IoMT) becomes more pervasive, type approval will require involvement of additional capabilities and authorities.

Given the expected growth of IoT devices, regulators will have to assign more spectrum in both licensed and unlicensed bands. At least in the near future, a significant proportion of IoT devices will use personal area networks (wi-fi) to access the internet (see Figure 4), and in multi-dwelling units and dense

urban areas, many people are already experiencing degradation of their wi-fi connections. In addition, with more rich content being consumed, the demand for high bandwidth in personal-area networks is going to increase exponentially. Recognizing the need for additional spectrum for wi-fi, the US Federal Communications Commission (FCC) recently issued “Notice of Inquiry”, seeking comments from the industry for allocation in 5.925–6.425 GHz (close to the existing 5 GHz wi-fi bands) and 6.425–7.125 GHz. Wifi.org, in its study¹, estimated an additional spectrum requirement of between 500 MHz and 1 GHz in various world regions to support expected growth in wi-fi by 2020. In addition, there are many low-powered IoT applications using wide-area technologies, for which spectrum in the lower band would be more suitable. In response to this, a few regulators are going as far as to reserve spectrum for IoT usage.

Figure 4: IoT devices by connecting technology, globally, 2015-2021



Source: Statista and Arthur D. Little analysis

2. Switching & roaming: No lock-in?

Integrated deployment of IoT devices at scale risks large customers being locked in with specific technologies, operators or service providers – if over-the-air remote provisioning is not implemented. Telecom regulators will have to decide under what circumstances they would mandate over-the-air remote provisioning, and how portable contracts should be. In addition,

¹ <https://www.wi-fi.org/beamon/alex-roytblat/wi-fi-study-reveals-need-for-additional-unlicensed-spectrum>

issues emanating from IoT devices running on “permanent” roaming bases will be more prevalent – for example, a car that ships with an embedded SIM on a global roaming plan. There will be implications from local and regional “know-your-customer” laws, and from ensuring reliability of services to the customers in the actual country where the IoT-linked service is provided and consumed.

Another issue for telecom regulators is whether to allow soft SIMs in the country, as many IoT devices will have form factors which will not allow them to accommodate physical SIMs. Embedded SIMs have been accepted by regulators and operators, but in future there may be a need for telecom regulators to evaluate a structured introduction of soft SIMs into the market, taking into account operators’ hesitancy regarding churn and concerns related to security.

3. Addressing & numbering: Beyond traditional services

The increased volume of IoT devices will drive up demand for numbering resources, in spite of a significant amount of devices expected on personal-area networks. Many regulators are already considering reserving specific number ranges for IoT usage. In many countries, pricing for numbering resources is based on unit revenue from traditional services, which is an order of magnitude higher than the unit revenue expected from many IoT services. Therefore, telecom regulators will also have to reassess the pricing of the numbering resources assigned for IoT usage based on much lower tariff and revenue assumptions.

In addition, IP-enabled IoT devices will require demand for networks to support IPv6 addressing, given the paucity of IPv4 addresses. At the moment, depending on the country, 25–60 percent of networks can support IPv6 addressing. Countries with lower readiness for IPv6 addressing may have to work with industry participants to facilitate early (and, in some cases, mandatory) moves to IPv6 addressing, and require future device deployments to be IPv6 compliant.

4. Competition: Technology-neutral

As IoT standards are still emerging, there is potential danger of not being able to derive benefits from the IoT if there is lack of interoperability from both data and technology perspectives. But there are a number of initiatives under way to facilitate interoperability through open-source developments. In 2014, IEEE initiated an effort to develop open standards for the IoT industry. However, as has been the trend in the past, regulators

are increasingly expected to remain technology neutral and allow market forces to decide the best technology standards to emerge.

5. Privacy & security: No compromise

IoT devices are already being used in both consumer and industrial contexts, including smart grids, building automation, and wearable computing. A US Federal Trade Commission report entitled “Internet of Things: Privacy & Security in a Connected World”² found that fewer than 10,000 households could generate 150 million discrete data points every day. This creates many more entry points for hackers and leaves sensitive information vulnerable. As technologies are still being developed and few industry-wide standards are in place, often products are launched into the market with old and unpatched embedded operating systems and software, which provide enough scope for potential hackers to access critical personal and industrial data. For example, German researchers were able to intercept unencrypted data from a smart-meter device to determine what television show someone was watching at that moment³.

In addition to security, privacy of individuals is at stake, as large amounts of personal data are being collected (which, at times, the user is also not aware of). The data is then sent across borders and stored and processed largely at the discretion of service providers. Consumers do notionally agree to terms of services, but very few read them. In many cases, such consent is mandatory for availing services, and often post hardware purchase, when the consumer is already effectively committed.

Given the increasing importance of data and the growing monetization of consumer data, allowing the industry to self-regulate may not be sufficient to protect consumers from abuse. This shifts the burden to policy-makers, with the added onus of not disrupting data-driven business models in their entirety.

How can policy-makers ensure consumer protection? Many countries do not have comprehensive regulations on data privacy and protection. In addition to regulations and legal frameworks, there are issues related to jurisdiction and implementation of legal rulings, as often the IoT service provider is based outside of the country.

National policy-makers will have to first define or adopt data management frameworks. The data management framework would define the data classification based on the extent of adverse impact on individuals from disclosure of their data. It would provide clear directions on data gathering, transmission,

2 <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>
 3 See Dario Carluccio & Stephan Brinkhaus, Presentation: “Smart Hacking for Privacy,” 28th Chaos Communication Congress, Berlin, December 2011, available at <https://www.youtube.com/watch?v=YYe4SwQn2GE&feature=youtu.be>.

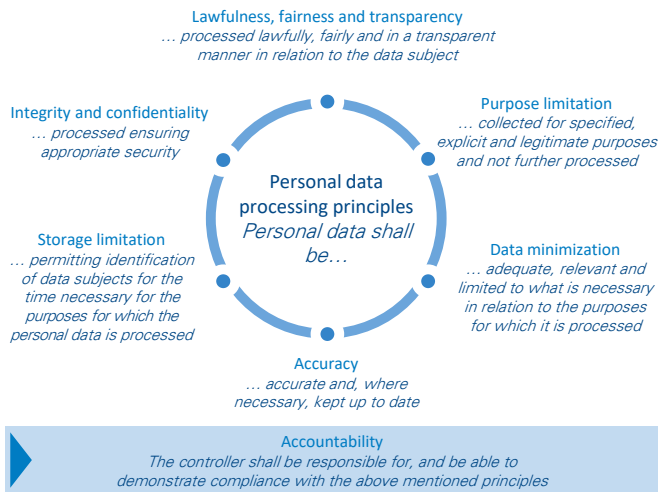
storage, processing and distribution. Some of the key questions a data management framework would address include:

- What data can be collected by IoT service providers, and what appropriate consent administration gets implemented between the stakeholders involved?
- How should the permissions sought be adopted based on data classification?
- How to ensure data breaches are reduced and, when breaches occur, consumers are notified about the same?
- How can policy-makers provide clarity to all IoT stakeholders on what data can leave the country and what cannot?

In addition to consumer privacy protection, there are concerns about preservation of national security. How can policy-makers ensure that IoT devices, especially the ones that are mass-deployed, are not illegally accessed and do not pose a significant threat to national security?

The regulation for personal data processing must fulfill six key principles (see Figure 5), including data minimization, storage limitation and integrity and confidentiality of data.

Figure 5: Personal data processing



Source: Arthur D. Little analysis based on EU Regulation 2016/679, article 5

Efforts are already under way: In order to address data protection issues for citizens and provide Europe-wide comprehensive and harmonized regulations for data protection, the European Parliament on 27th April 2016 issued the General Data Protection Regulation (GDPR) to protect natural persons with regard to the processing of personal data. (See Figure 6.) The regulation will come into effect in May 2018 within the European Union.

Figure 6: Requirements from target locations for transfer of data in EU GDPR1

- | | |
|---|---|
| <p>1 Level of protection of natural persons ensured in EU should not be undermined</p> | <p>4 In absence of an adequate level of protection, controller or processor to compensate for lack of data protection in target locations by way of appropriate safeguards for the data subject</p> |
| <p>2 High respect provided to the rule of law, access to justice and international human-rights norms and standards</p> | <p>5 Supervisory authorities² to have financial and human resources, premises and infrastructure necessary for effective performance of their tasks</p> |
| <p>3 Offer guarantees ensuring an adequate level of protection, essentially equivalent to that ensured within EU</p> | <p>6 Supervisory authorities² must perform awareness-raising activities addressed to the public</p> |

Source: Arthur D. Little

- 1) EU General Data Protection Regulation (GDPR) 2016/679 (27th April 2016)
- 2) One or more independent public authorities established by a Member State to be responsible for monitoring the application of EU GDPR regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing, and to facilitate the free flow of personal data

At a city level, New York recently issued guidelines for IoT⁴, and three out of five topics in these guidelines were data management, security and privacy.

Many countries are now contemplating developing data-privacy and security guidelines to address the challenges emanating from large amounts of personal data being generated and becoming available to IoT service providers. As it stands, consumers have limited ability to influence how their data is used.

⁴ <https://iot.cityofnewyork.us/>

4. Sharing of public IoT infrastructure: The more the better

There is a need to develop a public policy defining the requirements for IoT infrastructure deployment and sharing in public places, such as traffic sensors. Policy-makers will have to decide the number of parameters, including standards to use, points of interconnect, services to be made available to private players, and the mode of public-private partnership. By allowing greater use of IoT infrastructure, policy-makers can foster the rapid growth of IoT ecosystems in countries.

In addition, the state should publish clear guidelines as to where and how IoT infrastructure will be rolled out in public areas, and

also provide information to other potential participants about the availability of such infrastructure. There is also need for mechanisms whereby citizens can express their reservations if the deployment of IoT infrastructure in their vicinities adversely affects them.

Therefore, civic authorities have a critical role to play in the growth of their IoT ecosystems – similar to the role they are expected to play in providing open data.

5. How ICT regulators can lead with holistic frameworks

Policy-makers already appreciate the strong socio-economic benefits to be realized if the above concerns can be addressed and tackled effectively. But the IoT has largely been unregulated so far, and is developing on its own, with many countries addressing IoT-specific requirements on a case-by-case basis. Some countries are at a relatively more advanced stage, and are conducting detailed consultations on key aspects related to the IoT.

A clear regulatory framework can accelerate development of an IoT ecosystem and make it more sustainable, through the following key benefits:

- Accelerate development of the ecosystem through progressive market stimulation, such as increasing market clarity and promoting entrepreneurship
- Enhance national security through increased security of the overall ICT environment
- Enhance protection of rights and interests of users (individuals, enterprises and government)

Foundation: Clarity in context, vision and objectives

To achieve benefits, clear articulation of the country's or region's context, vision and objectives is essential. Different countries are adopting different options in line with their contexts, visions and objectives. At times the choices along various options can be in contradiction with achieving some of the defined objectives. However at an overall level, clearly defined visions and objectives enable development of comprehensive and coherent frameworks, which can then accelerate the development of sustainable IoT ecosystems.

The IoT regulatory framework can be designed with intent to intervene in market development in a minimal manner. IoT use

cases can be classified based on a number of criteria, including industry verticals and criticality of use cases.

Evolutionary approach on regulating use cases: The IoT is a big opportunity, but there are uncertainties for IoT ecosystem stakeholders. As it is an enabler of a large number of use cases, developing ex-ante regulations is not fully possible, given that the use cases are still evolving and the impact can be assessed only after they have been deployed. Therefore, it is critical that IoT regulation follows a use case-based, "evolutionary" approach, and that the framework is updated regularly as new use cases develop.

Lead and coordinate policy: ICT regulators need to provide clarity on many of the areas outlined above and where they have direct authority. As IoT devices will be used in a range of industries and have varied levels of complexity, telecom regulators will have to work with other ministries, regulators, and government bodies to effectively manage the growth of their IoT ecosystems.

Committed implementation: From an implementation perspective, the above designed IoT framework would rely on the following three key pillars, with the process potentially iterative – that is, as the IoT ecosystem developed further, the regulations would be updated accordingly:

- Development of IoT-specific, telecom-related regulatory policies and processes
- Development of national-level data management and protection guidelines
- Cross-industry governance structure

Conclusion

The IoT is proliferating and rapidly transforming the way individuals, enterprises and governments communicate and work. There will be a fundamental shift in lifestyles on the back of a large number of devices communicating with one another, and this will collaboratively result in increased optimization and enhanced productivity.

This expected large-scale deployment provides policy-makers with an opportunity to positively impact socio-economic development by steering and accelerating development of the IoT ecosystem. However, it also creates concerns about protecting the safety and privacy of users and preserving national security.

Faced with this dichotomy, successful policy-makers will be those that can identify the right level of regulation and lead in cross-sector coordination. While identification of this level would be a function of the areas that have been established and the options that have been chosen within each, a significant part in this success or failure would also be played by the governance mechanism defined to implement these regulations in the market. Following the implementation of a first set of regulations, the swiftness around assessing the created impact, and making corresponding periodic adjustments as required, will be the ultimate success factors in development of a progressive and sustainable IoT ecosystem.

Notes

Contacts

If you would like more information or to arrange an informal discussion on the issues raised here and how they affect your business, please contact:

Austria

Karim Taga
taga.karim@adlittle.com

Italy

Giancarlo Agresti
agresti.giancarlo@adlittle.com

Sweden

Martin Glaumann
glaumann.martin@adlittle.com

Belgium

Gregory Pankert
pankert.gregory@adlittle.com

Japan

Shinichi Akayama
akayama.shinichi@adlittle.com

Singapore

Yuma Ito
ito.yuma@adlittle.com

China

Russell Pell
pell.russell@adlittle.com

Korea

Hoonjin Hwang
hwang.hoonjin@adlittle.com

Spain

Jesus Portal
portal.jesus@adlittle.com

Czech Republic

Dean Brabec
brabec.dean@adlittle.com

Latin America

Guillem Casahuga
casahuga.guillem@adlittle.com

Switzerland

Clemens Schwaiger
schwaiger.clemens@adlittle.com

France

Julien Duvaud-Schelnast
duvaud-schelnast.julien@adlittle.com

Middle East

Lokesh Dadhich
dadhich.lokesh@adlittle.com

Turkey

Coskun Baban
baban.coskun@adlittle.com

Germany

Michael Opitz
opitz.michael@adlittle.com

The Netherlands

Martijn Eikelenboom
eikelenboom.martijn@adlittle.com

UK

Jonathan Rowan
rowan.jonathan@adlittle.com

India

Srini Srinivasan
srinivasan.srini@adlittle.com

Norway

Diego MacKee
mackee.diego@adlittle.com

USA

Sean McDevitt
mcdevitt.sean@adlittle.com



With the Internet of Things (IoT) everywhere, can regulation be far behind – How ICT regulators can enable IoT ecosystem development

Arthur D. Little

Arthur D. Little has been at the forefront of innovation since 1886. We are an acknowledged thought leader in linking strategy, innovation and transformation in technology-intensive and converging industries. We navigate our clients through changing business ecosystems to uncover new growth opportunities. We enable our clients to build innovation capabilities and transform their organizations.

Our consultants have strong practical industry experience combined with excellent knowledge of key trends and dynamics. Arthur D. Little is present in the most important business centers around the world. We are proud to serve most of the Fortune 1000 companies, in addition to other leading firms and public sector organizations.

For further information, please visit www.adl.com.

Copyright © Arthur D. Little 2018. All rights reserved.

www.adl.com/IoT_Policy