Leveraging the Internet of Things

S Ramadorai - Former Chairman of Tata Elxsi and Head of NSDC | Published: Oct 16 2014, 02:33 IST

SUMMARY *We need an institutionalised mechanism for IoT governance with representation from governments, businesses & civil society*

Hectic travel schedules are the bane of every business leader. Days and weeks on end being away from home base make long distance management a challenging affair. That might all be set for change in the near future given the growing pervasiveness of the 'Internet of Things'.

Imagine this. When you are travelling, the refrigerator in your house senses the low provisions based on a pre-programmed list of essentials and automates an order generation to the grocery store. The store acknowledges the order on your mobile and schedules a pick-up time. The invoice amount is cleared from your bank with a click on your mobile app. This is not a movie fantasy but could be a reality very soon!

Welcome to the age of the 'Internet of Things', or IoT.

Having been in the industry for over four decades, I have had the good fortune of being a part of the three waves of disruption that computing and the internet have brought about, each of which has brought its own amazing transformations.

The first wave, the 'Internet of Computers', flattened the world, breaking down knowledge barriers, making 'One World' a reality. Next came 'Web 2.0' that revolutionised socialisation amongst humans making the concept of 'One People' a reality. Now, we stand on the verge of a new wave of change transforming the plethora of devices in our physical world into a seamless extension of ourselves. IoT is making the concept of 'One Entity' a reality. We are in the age of any-time, any-place for any-one, to any-time, any-place for any-thing.

At the core of IoT is to bring together people, data, process, and objects or things, and connect them to communicate smartly taking the user experience to a different level altogether. It also raises fundamental questions around geographical boundaries that determine our legal systems, and issues of personal privacy.

There are already more connected devices than people on the planet. According to a Gartner report, by 2020, there will be as many as 26 billion connected devices on this planet. A consequence of networked things is smarter processes and services, which can support our economies, environment and health.

Of course, this means that businesses have the opportunity of working smartly. Here's an example touted as the 'best example yet of IoT'. When a defect was identified with Tesla's Model S Sedan which required a software update, instead of recalling 29,000 units, Tesla just pushed the software updates to each of its cars which were connected over the network, thus saving costs and damage to brand.

Another example is of companies like GE Aircraft Engines who provide enhanced services like predicting potential maintenance needs or identifying any abnormalities in performance and relay the same to on ground staff of the airlines, thus minimising any downtime on aircraft arrival.

Having established IoT's business advantages, perhaps we must look at the developmental challenges, especially from the perspective of emerging economies. For countries like India which are largely agrarian, IoT can impact productivity through soil data through sensors, and meteorological data on rainfall. In the utilities sector usage analysis and prediction results in smart networks can result in substantial resource savings. However, these technologies will need to be low-cost and affordable for a scalable solution.

Another critical area is healthcare. IoT would enable a connected, cost-effective, easy-to-use, healthcare system that would focus on preventive measures rather than curative, facilitating monitoring of patients remotely, cutting down the number of visits to hospitals.

In the famous movie Casino Royale, James Bond saves himself after a cardiac arrest by a health monitoring device which connects to a medical team which remotely gives him instructions and treatment. This could be a reality.

Most developing countries lack the software background and the capability to integrate the physical world to the digital world. Organisations like TCS specialise with a combined capability of the equipment and how to sense data and also in developing Big Data and Analytics around it to manage the 'remote diagnostics' part.

Many countries are pushing the envelope on leveraging IoT. As per the Global Information Technology report 2014 published jointly by INSEAD, Cornell University and World Economic Forum, the countries leading the Networked Readiness Index are the Netherlands, Switzerland, the US and the UK. London's Heathrow is all set to become the first airport in the world to use IoT technology to re-wire the experience of catching a flight.

While the US and Europe are moving ahead, China is establishing its leadership as well. A dedicated unit called China Mobile Internet of Things Ltd has been established to develop IoT and three verticals in particular are being focused upon—energy, transport and smart cities. The future of IoT raises two important questions—security and governance. But even before that, it is important to be sensitised with some other related issues.

Due to multiple entities involved in IoT, it is important to understand as to who owns your private data and who has the right to monetise it.

Interoperability is the first basic challenge as IoT involves different technologies and systems, so it is important to have one standard approach. As devices are spread across numerous locations, it will be difficult to ensure the operation, remote management and updating these devices. Data processing, networking and storage will consume enormous amounts of energy, and disposal of devices which are not very easy to recycle will be a challenge. So there are environmental issues to think about.

Security

With modern cryptanalysis advances, there is a certain minimum ‘key size’ and ‘algorithm complexity’ requirement needed to secure the devices from any malicious attack—as the devices used in IoT are so small (CPU, RAM or power) that most of these techniques are not really suitable to use, making them susceptible to data leaks. IoT can have multitude of devices across technologies including old archaic mainframe devices connected to new sensors. If a security issue is found in such a device, it is likely that the thousands of already deployed, in-the-field, devices will remain un-patched due to a variety of reasons like connectivity, size, etc. In fact, sustained support of this nature may be cost-prohibitive for the manufacturer.

Governance

Unfortunately, governance, regulations, ethical code of behaviour with regards to privacy and data have lagged behind the technology development. IoT is only exacerbating this problem. With cybersecurity on the rise, we need to step back and formulate global governance norms. We need to find answers to basic questions like—Who owns the data? Who has stewardship of the data? Who determines what data standards are to be set, where is the data to be kept? Who has access to the data? Who has the rights to monetise it? IoT involves interconnected devices, hence questions also arise about where and in which device does the data reside? Unfortunately, there is no black and white answer to these questions.

We need to set in motion an institutionalised mechanism for IoT governance with representation from governments, businesses and civil society. This is the right time to propose the idea of an International Cyber-Treaty Organisation (ICTO) that would set up ‘rules of the road’ for international cooperation on crime, together with an appropriate fund to finance cooperation as needed; ‘rules of the road’ and a process to assess when a country has gone over the line in acts of cyber-war, together with an appropriate sanctions regime; and a ‘privacy bill of rights’ for citizens worldwide that prevents unwarranted intrusion into their private lives.

Technology, used responsibly, can be both an accelerator and an enabler for the world of tomorrow. It provides new opportunities to foster innovation that boost economic and social prosperity of developed and emerging economies. To enable this for the future we need to begin with our schools and the education system. We should, like several countries are already doing, introduce into the curriculum coding and programming skills in an interesting and engaging manner. We also need to build curriculum that teaches our children ‘cyber ethics’ in our schools so that we raise responsible netizens of the future. Education and skilling will have to keep pace with tomorrow’s needs if the Indian economy is to enjoy sustained growth.

The author is chairman, NSDA and NSDC