

India must get on the IoT highway fast

Though Internet of Things throws up several data privacy challenges, India must push ahead

TV RAMACHANDRAN

Over 30 billion 'smart' devices will be connected by 2020. That's equivalent to every single person on this planet with not one, but four connected devices. These devices that communicate with each other in real time are known as the Internet of Things or IoT.

IoT is the natural evolution of the internet and has many benefits including boosting global economies, improving public utilities, and increasing efficiencies.

However, along with greater transparency and connectivity comes a potential risk to privacy. Nine out of 10 global consumer IoT brands studied in an IoT Security Foundation report (IoTSF) did not allow researchers to share findings about the vulnerabilities they found. This concern over data protection will need to be addressed. World over, legislators, device manufacturers, and law enforcement are coming together to figure out how to benefit from IoT while mitigating risks.

The Indian government outlined a plan to leverage IoT as part of the Digital India mission. There is a ₹7,000-crore budget to develop 100 smart cities, conserve water and power, and improve healthcare, transportation, and security.

Indian IoT market is expected to reach \$15 billion by 2020 and constitute 5 per cent of the global market (Nasscom). Investing in IoT will boost our economy on par with global leaders. IoT will bring in investments, create jobs and improve Indian public infrastructure. Tata Communications allotted \$100 million in IoT focusing on smart cities, utilities, and safety of people. Indian VC — Blume, created a \$100-million investment fund for IoT start-ups. MG Motors and Cisco recently announced their bid to launch connected cars

parts have already begun reaping the rewards of investing in IoT-based infrastructure. South Korea in particular made early investments in IoT and South Korean businesses are experiencing higher revenues of as much as \$7.16 billion.

Sweden boasts of being the world's most cashless society. With a network of inter-connected devices, their residents carry minimal cash, thereby increasing efficiencies and personal security. A city in Austria increased driver efficiency and reduced carbon dioxide emissions by about 500 tonne through connected trams and buses. The city of Oakland, California, tracks air pollution at a hyper-local level and can take measures to combat it.

Connectivity benefits

There are a lot of benefits associated with increased connectivity. Imagine being able to review the inventory in your fridge and order groceries remotely at the click of a button. IoT could help the elderly move around in self-driving cars, shop, and receive timely assistance. Japan is already using humanoid smart robots as elder care robots. Apart from monitoring their assigned senior citizen, they also assist with mobility, entertainment and rehabilitation.

There are significant leaps made in the world of healthcare as well with patient monitoring, voice-enabled systems to remind people to take their medication and a 'smart' pill that measures variables as the pill passes through your digestive system!

While IoT technology is clearly of significant advantage to citizens worldwide, IoT manufacturers will have to build and sustain consumer trust in their devices. IoT devices collect and share personal data in real-time, how can we protect our information and privacy? Particularly, as in the near future, IoT may be a default



Future's here Internet of Things can boost economies and improve delivery of public utilities ISTOCK.COM/JAMESTEOHART

Consumers may soon be unable to avoid IoT devices.

There is growing concern about the potential for increased government surveillance and a resulting encroachment of civil rights to suppress dissent or marginalise communities. Additionally, the annual cost of cyber crime is over \$1 trillion. Processing the tremendous amount of real-time IoT data is possible through artificial intelligence or AI algorithms. If AI powers essential functions of smart cities, how can we prevent hackers and miscreants from accessing and manipulating our data?

How can we address these concerns without hampering progress? It will need a higher level of cooperation between nations on a global scale. Policy-makers, regulators, device manufacturers, supporting industries and service providers will all have to join hands in creating a safer space online.

The state of California in the US just passed the first IoT Cybersecurity law that holds IoT device manufacturers to higher security standards. There is a discussion

published guidelines and codes for IoT manufacturers. The Internet Society's Online Trust Alliance (OTA) Trust Framework provides strategic principles to increase the security of IoT devices and data.

Indian angle

In India, the NDCP (National Digital Communications Policy) brought alignment from critical stakeholders to advance India's infrastructure and security around digital communications. MeitY's draft IoT policy seeks to establish committees to govern and drive IoT-specific initiatives.

It is not yet clear how much access to personal data these committees get and how their actions will be monitored. The Data Protection framework submitted by the Justice Srikrishna Committee earlier this year had some provisions for personal data protection including a consumer's right to information, consent, and right to request companies to erase their data if preferred.

However, it leaned heavily towards greater regulations and did not specify how to protect con-

Close on the heels of any policy-making is the debate around consent. Several regulations across the world indicate that IoT companies need to collect user consent prior to collecting the said data. However, in this extremely inter-connected world of data-sharing, there is a debate around how best to communicate and receive consent for personal data collected.

Despite the challenges, India must drive full speed ahead towards IoT technology for the greater good of our citizens. With effective global alliances and Indian stakeholder alignment, we can work to create more secure devices and help our citizens.

I dream of the day when a smart ambulance saves lives through timely medical intervention. Or a day when criminal behaviour is curbed through remote monitoring. I hope for a day soon when we can breathe clean air in our nation's Capital through smart control of the biggest generators of air pollution — and all these and more are possible through IoT.

The writer is President of Broadband