Internet of Things

What is the issue?

\n\n

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

\n\n

What is the Internet of Things?

\n\n

\n
- The Internet of things (IoT) is the network of devices, vehicles, and home appliances that contain electronics, software, actuators, and connectivity which allows these things to connect, interact and exchange data.
\n
- IoT involves extending Internet connectivity beyond standard devices, such as desktops, laptops, smartphones and tablets to everyday objects.
\n
- These objects may be anything from cell phones, coffee makers, washing machines, headphones, lamps, wearable devices.
\n
- It can also be components of machines, for example a jet engine of an airplane or the drill of an oil rig.
\n
- Embedded with technology, these devices can communicate and interact over the Internet, and they can be remotely monitored and controlled.
\n
- Thus, it is all about connecting devices over the internet and letting them ‘talk’ to us, applications and each other.
\n
- However, Internet of Things doesn’t necessarily have to be connected to the internet; it can also be a network of things.
\n

\n\n

What is the case with India?

\n\n

\n

- IoT is the natural evolution of the internet and has many benefits including boosting global economies, improving public utilities, and increasing efficiencies.
\n
- Many of our global counterparts have already begun reaping the rewards of investing in IoT-based infrastructure.
\n

\n\n

\n

- The Indian government outlined a plan to leverage IoT as part of the Digital India mission.
\n
- Indian IoT market is expected to reach $15 billion by 2020 and constitute 5% of the global market.
\n
- Investing in IoT will boost our economy on par with global leaders and it will also bring in investments, create jobs and improve Indian public infrastructure.
\n

\n\n

What are the concerns?

\n\n

\n

- IoT devices collect and share personal data in real-time, thus raising concerns on protecting personal information and privacy.
\n
- There is growing concern about the potential for increased government surveillance and a resulting encroachment of civil rights to suppress dissent or marginalise communities.
\n
- Additionally, the annual cost of cybercrime is over $1 trillion.
\n
- Since the IOT is capable of processing the tremendous amount of real-time data, it is possible for hackers and miscreants from accessing and manipulating those data.
\n
- Also, several regulations across the world indicate that IoT companies need to collect user consent prior to collecting the said data.
\n

- However, there is a debate around how best to communicate and receive consent for personal data collected.
  \n
- Thus, IoT manufacturers will have to build and sustain consumer trust in their devices.
  \n

\n\n

What should be done?

\n\n

  \n
- Policy-makers, regulators, device manufacturers, supporting industries and service providers will all have to join hands in creating a safer space online.
  \n
- The state of California in the US just passed the first IoT Cybersecurity law that holds IoT device manufacturers to higher security standards.
  \n
- The EU and the UK published guidelines and codes for IoT manufacturers.
  \n
- The Internet Society's Online Trust Alliance (OTA) Trust Framework provides strategic principles to increase the security of IoT devices and data.
  \n
- In India, the NDCP (National Digital Communications Policy) brought alignment from critical stakeholders to advance India's infrastructure and security around digital communications.
  \n
- The draft IoT policy seeks to establish committees to govern and drive IoT-specific initiatives.
  \n
- It is not yet clear how much access to personal data these committees get and how their actions will be monitored.
  \n
- The Justice Srikrishna Committee had recommended 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.
  \n
- However, it leaned heavily towards greater regulations and did not specify how to protect consumer data from unnecessary government surveillance.
  \n
- Despite these challenges, India must drive full speed ahead towards IoT technology for the greater good of our citizens.
  \n
- With effective global alliances and Indian stakeholder alignment, we can

work to create more secure devices and help our citizens.
\n

\n\n

\n\n

Source: Business Line

\n