ORIGINAL RESEARCH PAPER
Volume - 12 | Issue - 08 | August - 2023 | PRINT ISSN No. 2277 - 8179 | DOI : 10.36106/ijsr
INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH

WHY INDIA NEED CONSUMER INTERNET OF THINGS (IOT) DEVICES LEGISLATION; REASONS BEHIND

Law

Dr. Mamatha G.M Assistant Professor, School of Law, Presidency University Itgalpur, Rajanukunte, Yelahanka, Bengaluru-560064 (Karnataka State), India

SMD Azash Assistant Professor, School of Law Presidency University, Itgalpur, Rajanukunte, Yelahanka, Bengaluru-560064 (Karnataka State), India

Dr. Kayala Krishnamurty Associate Professor, School of Law Presidency University, Itgalpur, Rajanukunte, Yelahanka, Bengaluru-560064 (Karnataka State), India

ABSTRACT

While India has some existing laws that address aspects of data protection and cybersecurity, a specific legislation focused on the unique aspects of Consumer IoT devices can provide a more holistic and robust framework for ensuring the security and privacy of users in the rapidly expanding IoT ecosystem. Such legislation should strike a balance between promoting innovation and safeguarding consumer interests, enabling India to harness the full potential of IoT technology while protecting its citizens from potential risks.

KEYWORDS

Consumer, Data Protection, Internet of Things (IoT), Legislation, Privacy, Risk and Security.

INTRODUCTION

IoT / M2M technology is being used to create smart infrastructure in various verticals such as Power Sector, Automotive, Safety & Surveillance, Remote Health Management, Agriculture, Smart Homes and Smart Cities etc. The hacking of the devices/networks being used in daily life would harm companies, organisations, nations and more importantly people, therefore securing the IoT eco-system end-to-end i.e., from devices to the applications is very important.

An IoT network that has been compromised may result in the collapse of services, creating panic and chaos. Ensuring end to end security for connected IoT devices is key to success in this market -without security, IoT will cease to exist. Apart from security, the privacy of the data of the individuals is another very important domain, especially in sectors like health care. According to a market research report published by Markets and Markets, the global Internet of Things (IoT) security market size is expected to grow from USD 8.2 billion in 2018 to USD 35.2 billion by 2023, at a CAGR of 33.7 percent during the forecast period.

IoT devices, services & software, and the communication channels that connect them are at risk of attack by a variety of malicious parties, from novice hackers to professional criminals and even state actors. Possible consequences of such attacks could include:

- Discontinuity and interruption to critical services/infrastructure
- Infringement of privacy
- Loss of life, money, time, property, health, relationships, etc.
- Disruptions of national scale including civil unrest.

For vendors, operators and suppliers, potential consequences may include loss of trust, damage to reputation, compromised intellectual property, financial loss and possible legal liabilities.

Data can be leaked by malicious actors taking advantage of poor design. Even the unintentional leakage of data due to ineffective security controls can also have dire consequences to consumers and vendors. Thus, IoT devices and services must have security designed-in from the very outset.

IoT Security Foundation (IoTSF) in its annual report on vulnerability disclosure(February 2021) has mentioned an improvement in vulnerability disclosure by the manufacturers from 9.7% in 2018 to 18.9% in 2020. Companies under survey were from North America, Asia and Europe.

This is of great concern as vulnerability disclosure is widely considered to be a baseline requirement due to its fundamental importance towards operational IoT security. This report has mentioned that only a few companies are working on vulnerability disclosure despite incoming laws and international standards. Thus, it is imperative that the providers of IoT products implement the vulnerability disclosure policy on priority.

ETSI has released ETSI TS 103 645 (V 2.1.2) in June 2020 on Cyber Security for Consumer Internet of Things: Baseline Requirements. It is having 13 basic principles. ETSI TS 103 645 has been adopted by the European Union (EU) as ETSI EN 303 645. ETSI TC CYBER is taking forward TS 103 701, which will set out test scenarios for assessing products against EN 303 645.

UK and Australia have released Code of practice for consumer IoT security in 2018 and 2020 respectively, and are having the similar guidelines as available in ETSI TS 103 645. The Cyber Security Agency of Singapore (CSA) has launched a voluntary cyber security labelling scheme for consumer smart devices to improve IoT security based on ETSI EN 303 6459. Infocomm Media Development Authority (IMDA) Singapore has released a technical specification, in November 2020, for residential gateways (IMDA-TS-RG-SEC) having some mandatory provisions. The USA has published a law in December 2020 "IoT Cybersecurity Improvement Act of 2020", mandating National Institute of Standards and Technology (NIST) to develop the standard and guidelines on the use and management of IoT. The guidelines mentioned in this Code of Practice are aligned with the Cyber Security for Consumer Internet of Things.

Concept of Internet of Things (IoT)

The Internet of Things (IoT) is a technology that connects various devices and objects to the internet, enabling them to communicate, collect data, and perform automated actions.

The Internet of Things (IoT) describes the network of physical objects— "things"—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet.

Types of consumers IoT devices

consumer IoT products that are connected to the internet and / or home network and associated services. A non-exhaustive list of examples is as given below:

- Connected wearable healthcare devices
- Smart cameras, TVs and speakers
- Connected children's toys and baby monitors
- Connected safety-relevant products such as smoke detectors, and door locks Connected home automation and alarm systems
- Connected appliances (e.g., washing machines, fridges)
- Smart home assistants
- IoT gateway for connecting the consumer IoT devices.

Why India needs and the importance of IoT legislation:

While IoT offers numerous benefits and has the potential to revolutionize various sectors in India, it also raises specific concerns that necessitate proper legislation. Here are some reasons why India needs and the importance of IoT legislation:

1. Privacy and Data Protection:

IoT devices collect and process massive amounts of data, often including personal and sensitive information. Legislation is crucial to ensure that companies and individuals using IoT devices comply with data protection laws, obtain explicit consent for data collection, and implement adequate security measures to prevent data breaches.

2. Cybersecurity:
With the increasing number of interconnected devices, the attack surface for cybercriminals expands. IoT legislation can enforce cybersecurity standards, ensuring that manufacturers and users take necessary precautions to safeguard devices from hacking and prevent malicious activities.

3. Interoperability and Standards:
IoT devices come from various manufacturers and use different communication protocols. Legislation can promote the development and adoption of common standards, fostering interoperability among devices. This will enhance user experience and encourage innovation within the IoT ecosystem.

4. Liability and Accountability:
IoT devices can cause harm if they malfunction or lead to undesirable outcomes. Legislation can define liability frameworks, specifying responsibilities for manufacturers, service providers, and users, ensuring that they are held accountable for any damages caused by IoT devices.

5. Spectrum Management:
IoT devices often rely on wireless communication, which requires well-managed spectrum allocation. Legislation can help in efficiently allocating and utilizing the limited radio frequency spectrum for IoT devices, avoiding interference and congestion.

6. Energy Efficiency and Environmental Impact:
Regulations can incentivize the development and use of energy-efficient IoT devices, reducing their environmental footprint and contributing to sustainability goals.

7. Consumer Protection:
IoT devices are becoming increasingly prevalent in everyday life, and consumers need protection from misleading claims, unfair practices, and poor-quality products. Legislation can ensure that IoT manufacturers and sellers adhere to consumer protection laws.

8. Ethical Use of Data:
Legislation can address ethical concerns related to IoT data usage, such as unauthorized surveillance, profiling, and discriminatory practices. It can define ethical guidelines for data handling, usage, and sharing.

9. Smart City Implementation:
As India moves towards building smart cities, IoT will play a pivotal role in various infrastructure and service domains. Legislation can provide a legal framework for the safe and effective implementation of IoT technologies in smart city projects.

10. Economic Growth and Innovation:
A clear regulatory environment can instill confidence in investors and businesses, promoting IoT adoption and stimulating innovation in the IoT industry. This, in turn, can lead to economic growth and job opportunities.

Consequences of IoT Security Breaches
As the IoT ecosystem becomes increasingly interconnected and pervasive, the impact of security incidents can be far-reaching and severe. Some of the key consequences of IoT security breaches include:

1. Disruption of Critical Services and Infrastructure:
Many IoT devices are integrated into critical infrastructure systems, such as power grids, transportation networks, and healthcare facilities. An attack on these devices or networks could lead to service interruptions, posing significant risks to public safety and essential services.

2. Privacy Infringement:
IoT devices often collect and process vast amounts of personal and sensitive data. If these devices are compromised, malicious actors can gain unauthorized access to sensitive information, leading to privacy violations and identity theft.

3.Financial Loss and Fraud:
IoT devices that manage financial transactions or control smart home security systems can be targeted by cybercriminals to steal money, conduct fraudulent activities, or manipulate smart home environments for malicious purposes.

4. Compromised Safety and Health:
In sectors like healthcare, a security breach in IoT devices used for remote health management can have life-threatening consequences if medical data or treatment plans are altered maliciously.

5. Disruptions on a National Scale:
Large-scale IoT attacks could lead to civil unrest and widespread panic if essential services, communication networks, or transportation systems are compromised.

6. Loss of Trust and Reputation Damage:
IoT vendors, operators, and suppliers can face severe consequences if their devices or services are involved in security breaches. Loss of trust from consumers and businesses can lead to a decline in sales, a damaged reputation, and loss of market share.

7. Intellectual Property Compromise:
Attacks on IoT devices may result in intellectual property theft or reverse engineering of proprietary technology, leading to significant financial losses for companies.

8. Legal Liabilities:
IoT manufacturers and service providers may face legal liabilities and lawsuits from individuals and organizations affected by security breaches if they are found to be negligent in implementing proper security measures.

Significance of end-to-end security for IoT devices and networks
Indeed, securing the Internet of Things (IoT) ecosystem is of paramount importance to ensure the widespread adoption and success of IoT technologies across various sectors. As IoT devices become increasingly interconnected and play a significant role in critical infrastructure, industries, and daily life, the potential consequences of security breaches and privacy violations become more severe.

1. Protection from Cyberattacks:
With the increasing number of IoT devices and their connection to the internet, the attack surface for cybercriminals widens. Hackers could exploit vulnerabilities in IoT devices and networks to gain unauthorized access, compromise data integrity, or launch large-scale attacks that may lead to service disruption, financial losses, or even physical harm.

2. Ensuring Data Privacy:
IoT devices often collect and process sensitive data, such as personal health information, location data, and usage patterns. Maintaining data privacy is crucial to protect individuals from potential misuse or unauthorized access to their personal information.

3. Preserving Service Continuity:
Many IoT applications and services are integral to critical infrastructure, such as power grids, transportation systems, and healthcare. A security breach in these systems can lead to service disruptions, causing panic, chaos, and even jeopardizing public safety.

4. Building Trust and Confidence:
If users and businesses do not have confidence in the security of IoT devices and networks, adoption rates may suffer. Trust is vital for the growth of IoT technologies, as users need assurance that their data is safe and that the devices they use are not compromised. To address these challenges, several measures are being taken in the IoT industry:

Secure Design and Development:
Manufacturers are increasingly incorporating security features into IoT devices from the design phase itself, such as encryption, secure boot, and over-the-air updates. Security standards and certifications are also being developed to guide manufacturers in creating secure IoT products.

Authentication and Access Control:
Implementing robust authentication mechanisms and access controls ensures that only authorized users and devices can interact with IoT systems.

Data Encryption:
Encrypting data at rest and during transmission helps safeguard sensitive information from unauthorized access.

Security Patching and Updates:
Regularly issuing security patches and updates for IoT devices is essential to address newly discovered vulnerabilities and enhance device security.

IoT Security Platforms:
Companies are developing specialized IoT security platforms that monitor, detect, and respond to potential threats across IoT networks.

Regulatory Measures:
Governments and regulatory bodies may introduce legislation and guidelines to enforce IoT security standards and ensure compliance.

Legislations Pertaining to IoT in India
Technology has brought and continued to bring many changes in society at a rapid rate. In no time, it seems we are making the transgression to the world of artificial intelligence and 5G technology. The green shoots of the future are already visible if we know where to look.

The field of law is not adrift from this highly technologically dominated and globalized world. It is extremely easy to surf for a particular provision of law on the internet. Thus, technology has become an integral part of the legal field. Law and technology are interlinked and complement each other brilliantly. Technology is used to apply, execute, or study law, and law to regulate the use of technology.

Cybersecurity and Compliance Legislations in India
Cybersecurity is the practice of protecting computers, servers, mobile devices, electronic systems, networks, and data from malicious cyber-attacks. The National Cyber Security Policy, 2013 also lays down that protection of information infrastructure and preservation of confidentiality, integrity, and availability of information in cyberspace is the essence of secure cyberspace.

The Indian legislators recognized the need for cyber-security and passed some laws, rules, and regulations that need to be followed by everyone who works on networks, computers, or the internet.

The Information Technology Act, 2000
The Information Technology Act, 2000 (hereinafter referred to as the **"IT Act"**) is the complete code regulating and governing the use of Information Technology and cyber-based devices.

Section 43 of the IT Act lays down the penalty and compensation for damage caused to a computer, computer system, or computer network. This section is equipped to deal with the following instances, incidents, or situations:

- unauthorized accessing or securing of access to a computer, computer system, or computer network;
- damaging or causing damage to any computer, computer system or computer network, data, computer database, or any other programs residing in the computer, computer system or computer network;
- disrupting or causing disruption or any computer, computer system, or computer network;
- denying or causing the denial of access to any person authorized to access any computer system or computer network by any means;
- assisting any person to facilitate access to a computer, computer system, or computer network;
- charges the services availed of by a person to the account of another person by tampering with or manipulating any computer;
- destroying, deleting, or altering any information residing in a computer resource or diminishing its value or utility or affecting it injuriously by any means; or
- stealing, concealing, destroying, altering or causing any person to steal, conceal, destroy or alter any computer source code used for a computer resource to cause damage.

Section 43A of the IT Act makes a corporate body liable to pay compensation for failure to protect their data. Section 70B (7) lays down that if an intermediary fails to report to the Indian Computer Emergency Response Team (hereinafter referred to as **"CERT-In"**), it may be punished with imprisonment or a fine. These are important rules that aim to deal with cyber-attacks and lay down mechanisms to ensure cyber-security.

Information Technology (Intermediaries Guidelines) Rules, 2011
The government amended the Information Technology (Intermediaries Guidelines) Rules, 2011 (hereinafter referred to as the **"IT Rules"**) in 2018 with the aim to make internet security more stringent. The IT Rules also require the companies having more than 5 lakh users to have an office in India duly registered under the Companies Act, 2013 and an appointment of a nodal officer who will be able to work with the legal enforcement.

Though these rules don't have a direct connection with the IoTs, these make companies more accountable and responsible for their content.

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
The Computer Emergency Response Team- India, a functional organization of the Ministry of Electronics and Information Technology, Government of India, lay down cyber-security as its key objective. The IT Act, of 2000 designated CERT-In to serve as the national agency to perform the following functions in the area of cybersecurity:

- collection, analysis, and dissemination of information on cyber incidents;
- forecast and alerts of cybersecurity incidents;
- emergency measures for handling cybersecurity incidents;
- coordination of cyber incident response activities; and
- issue guidelines, advisories, vulnerability notes, and whitepapers relating to information security practices, procedures, prevention, response, and reporting of cyber incidents.

IoT and Intellectual Property Laws
IoT manufacturers are starting to get inclined towards licensing and protecting their innovation rights to ensure their designs and developments. There have been discussions over the patentability, copyright, and infringement of IoT for quite a while now. In the current times, to offer better IoTs, the manufacturers need to associate together with the numerous gadgets that are in use with the help of some standard technologies that exist.

The number of IoT patents filled in India has increased from 74 in 2009 to 1,820 in 2017. In the landmark judgment by Delhi High Court in the case between **Ferid Allani v. Union of India**, the Intellectual Property Appellate Board relied on Section 3(k) of the Indian Patents Act, 1970.

Provisions of Law of Contracts
With the evolution of IoT devices, customers can enter into contracts for the sale of goods in a Machine-to-Machine mode (also known as "M2M"). This form of contract is referred to as a Smart Contract. There are no provisions in the Indian Contracts Act, 1872 to govern IoTs.

Data ownership, security, and privacy in an IoT environment can be reasonably addressed by contracts between device manufacturers or/ and IoT service providers and IoT users. These contracts may be entered by way of End User Licensing Agreements (herein referred to as EULA) governing the terms and conditions of use of the software or device.

Data Protection Laws
India did not have any laws governing data protection and ensuring data privacy. In June 2017, a committee was set up to study issues related to data protection. The committee formulated a Draft Personal Data Protection Bill, 2018 and after various deliberations and amendments, the Cabinet approved the bill on 4th December 2019 as the Personal Data Protection Bill, 2019. (Hereinafter referred to as the **"PDP Bill"**)

The framework of the PDP Bill lays down requirements of taking informed consent of the data subject before collecting or sharing data. It lays down explicit purposes for which the personal data collected will be used, destructing of data after the purpose has been fulfilled, etc.

The Bill seeks to address the core concern of data privacy but does not

take into account the practical enforceability of it in IoT-enabled environments. It is very difficult to determine the exact purpose of data collection beforehand in an environment where the uses for the same datasets are constantly evolving.

The PDP Bill 2019, though well-intentioned and in the right direction to protect data privacy and give control of own data to the data subject might not be best suited for IoT devices. However, it still plays a key role in addressing one of the core concerns of privacy.

CONCLUSION

Consumer IoT devices often collect and process personal data, such as location information, health data, and behavioural patterns. The number of IoT devices in the consumer market is increasing exponentially, ranging from smart home devices, wearables, and connected appliances. With the growing adoption of these devices, it also poses many challenges such as vulnerable to cyberattacks due to factors like poor security design, lack of regular updates, and weak authentication mechanisms. The data embedded in Consumer IoT devices is highly sensitive and requires specific regulations to ensure it is protected from unauthorized access, misuse, and exploitation. Legislation can enforce security standards, encouraging manufacturers to prioritize security in their devices.

REFERENCES

1. Krishna, Vishal. "India's IoT Started out Slow, but It's Time to Pick up Pace." YourStory.com, Yourstory, 27 Aug. 2018, yourstory.com/2018/08/indias-iot-started-slow-time-pick-pace.
2. "Unlocking the Potential of the Internet of Things." McKinsey & Company, www.mckinsey.com/ business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.
3. "Paul A. David, 1990, 'The Dynamo and the Computer: A Historical Perspective on the Modern Productivity Paradox', American Economic Review, 80(2), pp. 355–61."
4. Yueh, Linda. The Great Economists. Penguin Books Ltd., 2019.
5. Basulto, Dominic. "3 Reasons Why the Internet of Things (Still) Doesn't Make Sense." The Washington Post, WP Company, 16 Jan. 2015, www.washingtonpost. com/news/innovations/wp/2015/01/16/3-reasons-why-the-internet-of-things-still-doesnt-make-sense/?noredirect=on.
6. 6,7,20,33 Saleem, Jibran, et al. "IoT standardisation: Challenges, perspectives and solution." Proceedings of the 2nd International Conference on Future Networks and Distributed Systems. ACM, 2018.
7. Department for Digital, Culture, Media and Sport, UK government (2018). Secure by Design. Department for Digital, Culture, Media and Sport, UK government.
8. Fruhlinger, Josh. "The Mirai Botnet Explained: How IoT Devices Almost Brought down the Internet." CSO Online, CSO, 9 Mar. 2018, www.csoonline.com/article/ 3258748/ the- mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html.
9. Asplund, Mikael, and Simin Nadjm-Tehrani. "Attitudes and perceptions of IoT security in critical societal services." IEEE Access 4 (2016): 2130-2138.
10. "HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack." HP News – HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack, www8.hp.com/us/en/hp-news/press-release.html?id=1744676.
11. Meddeb, Aref. "Internet of things standards: who stands out from the crowd?." IEEE Communications Magazine 54.7 (2016): 40-47.
12. Pal, Arpan, et al. "IoT Standardization: The Road Ahead." Internet of Things-Technology, Applications and Standardization (2018): 53.
13. BlackBerry Survey Finds Consumers Don't Trust Connected Devices to Keep Data Safe and Secure, www.blackberry.com/us/en/company/newsroom/press-releases/2019/blackberry-survey- finds-consumers-don-t-trust-connected-devices-to-keep-data-safe-and-secure.
14. Andrukiewicz, E., Cadzow, S. and Górniak, S. (2019). IOT Security Standards Gap Analysis. [online] ENISA. Available at: https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis [Accessed 14 Jun. 2019].
15. "What Is the General Data Protection Regulation? Understanding & Complying with GDPR Requirements in 2019." Digital Guardian, 15 May 2019, digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection.
16. Digital. "Secure by Design Report." GOV.UK, GOV.UK, 7 Mar. 2018, www.gov. uk/government/publications/secure-by-design-report.
17. Towers-Clark, Charles. "UK To Introduce New Law For IoT Device Security." Forbes, Forbes Magazine, 2 May 2019, www.forbes.com/sites/charlestowersclark/ 2019/05/02/uk-to-introduce-new-law-for-iot-device-security/#1cb2147c579d.
18. Sync, CRM. "DCMS Launch Secure by Design Regulation Consultation." TechUK, TechUK, www.techuk.org/insights/news/item/15299-dcms-launch-secure-by-design-regulation-consultation.
19. Noor, Arshad. "California SB-327 and the Wake-Up Call for Stronger Authentication." CPO Magazine, 28 May 2019, www.cpomagazine.com/cyber-security/california-sb-327-and-the-wake-up-call-for-stronger-authentication/.
20. Robertson, Adi. "California Just Became the First State with an Internet of Things Cybersecurity Law." The Verge, The Verge, 28 Sept. 2018, www.theverge. com/2018/9/28/17874768/ california-iot-smart-device-cybersecurity-bill-sb-327-signed-law.
21. Ng, Alfred. "Congress Introduces Bill to Improve 'Internet of Things' Security." CNET, CNET, 11 Mar. 2019, www.cnet.com/news/congress-introduces-bill-to-improve-internet-of-things-security/.
22. Rash, Wayne. "IoT Security Bills for US Government Will Also Affect Business IT." EWEEK, 9 July 2019, www.eweek.com/security/iot-security-bills-for-us-government-will-also-affect-business-it.
23. Young, Mark. "European Parliament Approves EU Cybersecurity Act." Inside Privacy, 15 Mar. 2019, www.insideprivacy.com/international/european-union/european-parliament-approves-eu-cybersecurity-act/.
24. Panday, Jyoti. "India's Supreme Court Upholds Right to Privacy as a Fundamental Right-and It's About Time." Electronic Frontier Foundation, 11 Oct. 2017, www.eff.org/deeplinks/2017/08/indias-supreme-court-upholds-right-privacy-fundamental-right-and-its-about-time.