JOURNAL OF LAW, INFORMATION & SCIENCE
ISSN 0729-1485• Vol. 4, Issue 1 (2026) • https://jlisjournal.com/

REVIEW ARTICLE Article ID: JLIS/2026/4/1/013

Internet of Things and Cyber Law: Legal Challenges of Connected Devices in the Digital Society

Dr. Arjun Rao [1]

[1] *Department of Technology Law and Digital Security, Indian Institute of Legal Technology, Hyderabad, India.*

Received: 18 Nov 2025 **Revised:** 28 Feb 2026 **Accepted:** 28 April 2025 **Published:** 14 June 2026

ABSTRACT

The Internet of Things (IoT) has transformed the technological environment by connecting physical devices, sensors, vehicles, household appliances, healthcare systems, industrial equipment, and other objects to digital networks. Although IoT technologies provide significant benefits in automation, efficiency, monitoring, and data-driven decision-making, their widespread deployment creates complex legal and cybersecurity challenges. Connected devices continuously collect, process, and transmit large quantities of information, including potentially sensitive personal and behavioral data. Vulnerabilities in poorly secured IoT devices may expose users to unauthorized access, surveillance, identity-related risks, data breaches, and other forms of cybercrime. This article examines the intersection of IoT technology and cyber law, focusing on privacy, data protection, cybersecurity, device liability, digital evidence, consumer protection, and regulatory accountability. It argues that conventional legal frameworks may require technological adaptation to address the distributed and interconnected nature of IoT ecosystems. The article proposes a security-by-design framework incorporating encryption, authentication, software updates, access control, vulnerability disclosure, data minimization, and continuous monitoring. It concludes that effective IoT governance requires cooperation between technology developers, manufacturers, service providers, regulators, and users to establish a secure and legally accountable connected environment.

Keywords: *Internet of Things; Cyber Law; IoT Security; Data Protection; Privacy; Connected Devices; Cybersecurity.*

1. Introduction

The Internet of Things has become an important component of contemporary digital infrastructure. Devices that were previously independent and offline are increasingly connected to the internet and capable of collecting, processing, and exchanging information. Smart televisions, wearable devices, connected vehicles, smart cameras, medical equipment, industrial sensors, home-security systems, and smart-city infrastructure are examples of IoT technologies.

The growth of IoT has created substantial benefits. Connected devices can automate routine tasks, improve industrial productivity, facilitate remote healthcare, monitor environmental conditions, and enhance transportation systems.

However, connectivity also creates vulnerabilities.

A device connected to the internet can potentially become an entry point into a larger technological environment. If security controls are inadequate, attackers may exploit vulnerabilities to obtain information, manipulate devices, disrupt services, or access connected networks.

The legal implications of these risks are significant. Questions arise regarding who is responsible when an insecure IoT device causes harm, how personal information collected by devices should be protected, and what cybersecurity standards manufacturers should be required to follow.

This article examines these challenges and proposes a technology-oriented legal framework for responsible IoT deployment.

---

2. Concept of the Internet of Things

The Internet of Things refers broadly to interconnected physical devices capable of collecting, transmitting, receiving, or processing digital information.

An IoT ecosystem may contain:

- sensors;
- smart appliances;
- wearable devices;
- connected vehicles;
- industrial machines;
- surveillance cameras;
- medical devices;
- communication networks; and
- cloud platforms.

The architecture generally involves three broad components:

Device Layer: Physical devices and sensors collect information.

Network Layer: Communication infrastructure transfers information.

Application Layer: Software platforms process and interpret the information.

This interconnected structure creates both technological opportunities and cybersecurity risks.

3. IoT and Personal Data

Many IoT devices collect information about users and their behavior.

A smartwatch may collect information about movement and daily activity. A smart speaker may process voice interactions. A connected vehicle may generate information regarding journeys and vehicle usage.

Even when individual data points appear harmless, continuous collection can create detailed behavioral profiles.

This raises important privacy questions.

Organizations operating IoT services should consider what information is collected, why it is collected, how long it is retained, and who can access it.

Data minimization and purpose limitation can help reduce unnecessary privacy risks.

4. Privacy Risks

IoT devices can create privacy risks because they may operate continuously and sometimes with limited user awareness.

A traditional website interaction generally occurs when a user actively accesses a service. An IoT device, by contrast, may collect information automatically.

For example, connected cameras may continuously monitor an environment, while wearable devices may regularly transmit information.

The legal challenge is therefore to ensure that technological convenience does not result in excessive or invisible surveillance.

Users should receive understandable information about significant data-collection practices.

5. Security Vulnerabilities in IoT Devices

A major challenge is that many IoT devices have limited computing resources.

Some devices may operate with:

- weak authentication;
- outdated software;
- insecure communication protocols;
- default passwords;
- insufficient encryption; or
- limited update capabilities.

Manufacturers may also prioritize cost and functionality over long-term security.

Because IoT devices can remain operational for many years, vulnerabilities may persist after deployment.

Security therefore needs to be incorporated into the entire product lifecycle.

---

6. IoT and Cybercrime

IoT devices can become targets or instruments of cybercrime.

Attackers may compromise devices to:

- steal information;
- monitor users;
- disrupt services;
- conduct fraud;
- create botnets;
- access other systems; or
- manipulate physical processes.

The physical consequences can be particularly serious where IoT technology controls industrial or medical equipment.

Cyber law must therefore account for the connection between digital attacks and physical consequences.

---

7. Connected Vehicles

Connected vehicles represent an important example of the relationship between IoT and cybersecurity.

Modern vehicles may contain numerous sensors, communication systems, navigation technologies, and internet-connected services.

A compromised vehicle system could potentially affect navigation, communications, or other connected functions.

This raises questions concerning manufacturer responsibility, software updates, cybersecurity testing, data protection, and liability.

Vehicle manufacturers increasingly need to treat cybersecurity as a component of product safety.

---

8. IoT in Healthcare

IoT technologies have significant applications in healthcare.

Connected medical devices can monitor patients and transmit information to healthcare professionals.

Examples include:

- wearable monitoring devices;
- connected diagnostic equipment;
- remote patient-monitoring systems; and
- smart medical infrastructure.

However, healthcare-related IoT data can be highly sensitive.

A cybersecurity incident could simultaneously affect patient privacy and healthcare operations.

Healthcare organizations therefore require strong security architecture, access control, encryption, and incident-response mechanisms.

---

9. Smart Homes

Smart-home technologies provide another major IoT application.

Connected locks, cameras, thermostats, lighting systems, speakers, and appliances can be remotely controlled through digital platforms.

These devices may increase convenience but can also create security risks.

A compromised smart camera, for example, could potentially expose private household information.

Manufacturers should therefore provide secure authentication, regular security updates, and clear privacy policies.

---

10. IoT and Consumer Protection

Consumers may not possess sufficient technical knowledge to evaluate the cybersecurity of connected devices.

This creates an information imbalance between manufacturers and users.

Consumers may purchase devices without understanding:

- how long software support will continue;
- what information is collected;
- whether encryption is implemented;
- how vulnerabilities are reported; or
- whether the device can function securely after updates stop.

Consumer-protection frameworks may therefore require clearer disclosure concerning cybersecurity capabilities and support periods.

---

11. Manufacturer Liability

An important legal question concerns responsibility for insecure devices.

Suppose a manufacturer sells a connected device containing a serious vulnerability. If the vulnerability is subsequently exploited and causes harm, questions may arise regarding manufacturer responsibility.

Liability may depend upon factors such as:

- the nature of the vulnerability;
- whether the manufacturer knew about it;
- whether reasonable security measures were available;
- whether security updates were provided; and
- whether the user contributed to the incident.

Clear legal standards can encourage manufacturers to treat cybersecurity as an essential product requirement.

---

12. Security by Design

Security by design requires cybersecurity to be considered during product development rather than after a device is already deployed.

Important principles include:

Secure Authentication

Devices should avoid weak default credentials and support appropriate authentication mechanisms.

Encryption

Sensitive information should be protected during transmission and storage.

Secure Updates

Manufacturers should provide reliable mechanisms for delivering security patches.

Least Privilege

Devices and applications should receive only the permissions necessary for their functions.

Secure Configuration

Default configurations should prioritize security rather than convenience alone.

---

13. Software Updates and End-of-Life Issues

IoT devices may remain in use long after manufacturers stop providing security updates.
This creates a significant cybersecurity problem.
A device may continue functioning normally while containing vulnerabilities that can no longer be patched.
Manufacturers should therefore clearly communicate the expected security-support period.
For critical devices, long-term security support may be particularly important.
Legal and regulatory frameworks may also consider whether manufacturers should provide minimum security-support periods for certain categories of connected products.

---

14. IoT Supply-Chain Security

IoT products frequently contain components manufactured by multiple companies.
A device may include hardware from one supplier, software from another, communication services from a third party, and cloud infrastructure from another provider.
A vulnerability in any component can affect the entire ecosystem.
Organizations should therefore conduct appropriate supply-chain risk assessments.
Software-component inventories and vendor-security requirements can improve visibility.

---

15. Digital Evidence from IoT Devices

IoT devices can also become sources of digital evidence.
Smart cameras may contain video records. Connected vehicles may maintain location information. Smart devices may contain timestamps and activity records.
Such information may become relevant in criminal or civil investigations.
However, investigators must establish the authenticity and integrity of IoT-generated data.
Digital forensic procedures should therefore include appropriate acquisition, preservation, hashing, and documentation.

---

16. Artificial Intelligence and IoT

AI and IoT are increasingly being integrated.
IoT devices generate large amounts of information, while AI systems can analyze this information to identify patterns and make predictions.
For example, AI may analyze sensor information to identify equipment failures before they occur.
However, combining AI with IoT also creates additional risks.
Incorrect AI outputs may influence automated physical systems.

Therefore, high-risk IoT environments should incorporate human oversight, system testing, and fail-safe mechanisms.

---

17. Smart Cities

IoT technology is central to the development of smart cities.

Connected systems can monitor:

- traffic;
- public transportation;
- energy consumption;
- environmental conditions;
- water systems; and
- public infrastructure.

Smart-city systems can improve efficiency but may also create large-scale surveillance and cybersecurity concerns.

A successful attack against interconnected municipal infrastructure could affect multiple services simultaneously.

Smart-city governance should therefore incorporate privacy protection and cybersecurity from the planning stage.

---

18. Proposed Legal-Technological Framework

A comprehensive IoT governance framework should include the following elements.

18.1 Security by Design

Cybersecurity should be integrated into product development.

18.2 Privacy by Design

Personal information should be protected through system architecture.

18.3 Minimum Security Standards

Manufacturers should implement baseline security measures appropriate to device risk.

18.4 Vulnerability Disclosure

Users and security researchers should have clear mechanisms for reporting vulnerabilities.

18.5 Security Updates

Manufacturers should provide appropriate security support throughout the declared product lifecycle.

18.6 Incident Reporting

Significant cybersecurity incidents should be reported through appropriate institutional mechanisms.

18.7 Accountability

Clear responsibility should exist among manufacturers, operators, service providers, and other relevant participants.

---

19. IoT Governance Model

A practical governance model can be structured around four levels.

Level 1 – Device Security: Authentication, encryption, secure hardware, and secure configuration.

Level 2 – Network Security: Segmentation, monitoring, secure communication, and intrusion detection.

Level 3 – Data Governance: Data minimization, access control, retention management, and privacy protection.

Level 4 – Legal Governance: Regulatory standards, accountability, auditing, incident reporting, and consumer protection.

This layered model recognizes that IoT security cannot be achieved through a single technological mechanism.

---

20. Future of IoT Regulation

The IoT ecosystem will continue to expand as 5G, edge computing, AI, robotics, and autonomous systems become more widely adopted.

Future devices may become increasingly autonomous and interconnected.

This development will require legal frameworks capable of addressing complex questions of responsibility and cybersecurity.

Future research should examine liability for autonomous IoT systems, international cybersecurity standards, AI-enabled connected devices, biometric IoT systems, and cross-border data flows.

Technological regulation will need to remain sufficiently flexible to accommodate future innovation without compromising fundamental security principles.

---

21. Conclusion

The Internet of Things represents a major technological transformation in which physical objects increasingly interact with digital networks.

Connected devices can improve healthcare, transportation, manufacturing, home automation, public infrastructure, and numerous other sectors. However, the same connectivity creates new cybersecurity, privacy, and legal risks.

Weak authentication, inadequate updates, insecure software, excessive data collection, and poorly protected communication channels can expose individuals and organizations to significant harm.

The appropriate response is not to restrict IoT innovation but to establish a security-oriented technological and legal framework.

Security by design, privacy by design, encryption, secure authentication, vulnerability disclosure, software-update mechanisms, supply-chain security, and effective accountability should form the foundation of responsible IoT development.

Manufacturers, technology providers, infrastructure operators, regulators, and consumers all have important roles in maintaining a secure IoT ecosystem.

Ultimately, the future of connected technology will depend not only on how intelligently devices communicate but also on how securely and responsibly that communication occurs. A strong relationship between technological design and legal governance will therefore be essential for building a trustworthy and sustainable Internet of Things.

Declarations

Conflict of interest: The authors declare that they have no conflict of interest.

Funding: This review received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Ethical approval: Not applicable. This article is a review of published literature and did not involve human participants or animal subjects.

Data availability: No new data were generated or analyzed in support of this review. All sources relied upon are cited in the References.

Use of AI tools: No generative artificial intelligence tool was used in the conception, drafting or analysis of this article. The authors take full responsibility for the content.

Author contributions: Author contributed to the conception of the review, the survey of the literature, and the drafting and revision of the manuscript. Author read and approved the final version.