SNS COLLEGE OF TECHNOLOGY

Coimbatore-35

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A++' Grade

Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

19ECE306- SMART IoT APPLICATIONS

III ECE / V SEMESTER

UNIT 4– IOT LEGAL PERSPECTIVES AND STANDARDIZATION

TOPIC 4 –Responsibility for Violations of Privacy in IoT

Responsibility for Violations of Privacy in IoT

- 1. **Liability Issues -**In cases where privacy violations occur within the Internet of Things (IoT), individuals will likely seek accountability.
- This includes compensation for the violation and measures to prevent future breaches.
- Identifying who should be held liable in the IoT structure is crucial.
- On the Internet, liability often falls on service providers, particularly for hosting illegal content.
- The liability distinction lies between those offering access to the Internet and those hosting content.

Responsibility for Violations of Privacy in IoT

- Internet service providers (ISP), even if unaware of the content, may be held responsible alongside content creators due to the Internet’s architecture, which involves intermediaries controlling information flow.
- In the IoT, however, businesses will upload their own product-related information, and there will not be specific providers offering content hosting.
- While access providers exist, holding them liable for privacy violations committed by users is unjustified.

Responsibility for Violations of Privacy in IoT

- Providers cannot verify if users will engage in illegal activities, and servers may not have the capability or legal authority to control content effectively, especially when the content spans multiple jurisdictions with different regulations.
- Moreover, holding servers liable may lead to "over-blocking," as seen with ISPs on the Internet.
- To avoid liability, ISPs often resort to over-filtering objectionable materials, sometimes without valid reasons.
- This can result in censorship by commercial companies with the technical expertise to filter content, often without government oversight.

Responsibility for Violations of Privacy in IoT

- However, providers could be held liable if it is demonstrated that they had or should have had knowledge of the privacy violation.
- While it's unrealistic to expect providers to monitor all the information transmitted via their service, they should act upon discovering infringements.
- The level of attention providers need to pay to the users they grant access to the IoT will likely be evaluated on a case-by-case basis.
- Ultimately, the companies responsible for violating privacy rights must be held accountable, though identifying the violator and determining the jurisdiction can be complex.

Responsibility for Violations of Privacy in IoT

2. Education of Civil Society Beyond regulatory and technical measures, educating IoT users on security and privacy is critical.

- Proper education can mitigate risky behaviors among individuals and businesses.
- Education should go beyond explaining potential privacy breaches, focusing first on a comprehensive understanding of the IoT and its mechanisms.
- With this foundation, users can better protect themselves and comprehend security threats.

Responsibility for Violations of Privacy in IoT

- Education efforts should not only highlight isolated threats but also elucidate the patterns behind them.
- The delivery format should be accessible and simplify complex processes, acknowledging that while IoT users may be more knowledgeable than average Internet users (since businesses are the primary IoT participants), overestimating their understanding could be counterproductive.

Responsibility for Violations of Privacy in IoT

- The education must serve two purposes: teaching users how to interact safely within the IoT and enabling them to recognize potential risks or breaches.
- This awareness can prompt users to address threats or report them to relevant authorities, thereby enhancing the security and availability of the IoT.
- Educational programs should be flexible enough to adapt to evolving technology without requiring constant updates to materials.

Responsibility for Violations of Privacy in IoT

- A practical approach would be for businesses to appoint representatives who receive training from international IoT bodies.
- These representatives would stay updated on the latest privacy and security practices and be responsible for educating their colleagues..
- This method ensures ongoing knowledge transfer within organizations and maintains a high level of preparedness against privacy violations.