The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2024

Editor-in-Chief – Prof. (Dr.) Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

ONLINE PRIVACY AND CYBERSECURITY: CHALLENGES AND REGULATIONS

ABSTRACT:

Cybersecurity and online privacy are two essential components of a safe and secure online experience. This blog navigates the complex terrain of digital security and addresses potential cybersecurity threats, Exploring the challenges posed by evolving threats and the regulatory frameworks designed to safeguard sensitive information. This discussion unveils against the backdrop of high-profile data breaches, Targeted Ransomware cyber-attacks, and the daily development of the AI influence.

INTRODUCTION:

Cybersecurity and Privacy issues are becoming an important barrier for a trusted and dependable global digital society development. Cyber-criminals are continuously shifting their cyber-attacks specially against cyber-physical systems and IoT, since they present additional vulnerabilities due to their constrained capabilities, their unattended nature and the usage of potential untrustworthiness components. Likewise, identity-theft, fraud, personal data leakages, and other related cyber-crimes are continuously evolving, causing important damages and privacy problems for individuals in both virtual and physical scenarios. Consequently, this article aims to provide a comprehensive understanding of the crucial role of regulations in online privacy and cybersecurity.

ONLINE PRIVACY AND CYBERSECURITY:

- The definition of privacy incorporates two important elements: “the state of being alone and not being watched or interrupted by other people.”
- The online privacy is the level of privacy protection to an individual who has connected to the internet. It covers the amount of online security available for personal and financial data, communications, and preferences. Internet users often attempt to increase online privacy through anti-virus software, strong password choices, turning off tracking and option for stricter privacy setting.
- Cybersecurity is the protection to defend internet-connected devices and services from malicious attacks by hackers, spammers, and cybercriminals. The practise is used by companies to protect against phishing schemes, ransomware attacks, identity theft, data breaches and financial losses.

CHALLENGES:

1. **Potential of Artificial Intelligence (AI):** With AI being introduced in all market segments, this technology with a combination of machine learning has brought tremendous changes in cybersecurity. Artificial intelligence has been paramount in building automated security systems, natural language processing, face detection, and automatic threat detection. Although, it is also being used in develop smart malware and attacks to bypass the latest security protocols in controlling data. AI enabled threat detection systems can predict new attacks and notify admins of any data breach instantly.

2. **Targeted Ransomware:** Another important cybersecurity trend we can't seem to ignore is targeted Ransomware. Especially in the developed nations industries rely heavily on specific software to run their daily activities.\

3. **Data Breaches:** Prime Target: Data will continue to be a leading concern for organizations around the world. Whether it be for an individual or organization, safeguarding digital data is the primary goal now. Any minor flaw or bug in your system browser or software is a potential vulnerability for hackers to access personal information.

REGULATIONS:

1. **The Information Technology Act, 2000**

    - This Act was enacted by the Parliament of India and administered by the Indian Computer Emergency Response Team to guide cybersecurity legislation and govern cybercrime. India uses unitary cybersecurity law.
    - For example, in Section 43A, where a body corporate, dealing with any sensitive personal data is negligent in maintaining reasonable security practices and procedures and thereby causes wrongful loss to any person, such body corporate shall be liable to pay damages.

2. **Information Technology [Amendment] Act 2008**
    - These amendments helped improve the original bill which updated and redefined the terms by expanding the definition of cybercrimes and validation of electronic signatures. This Act applies to any individuals, company, or organization that uses computer resources which has over nine chapters and 117 sections.

3. **Information Technology Rules, 2011**
    - This rule aims to protect personal data which is collected by an individual or a person who is involved in commercial or professional activities. The most significant amendments include provisions for regulating intermediaries, violation fees for cybercrime, cheating, and other restrictions.

4. **National Cyber Security Policy, 2013**
    - The goal behind this policy is to create and develop more dynamic policies and to improve the protection of India's cyber ecosystem. This policy aims to create a robust framework and strategies for minimizing cyber incidents and cyber threats. It encourages organizations to develop cybersecurity policies that align with strategic goals.

5. **KYC [Know your customer]**
    - This has been mandated by the RBI, KYC is the tracking and monitoring of customer's data security to safeguard against fraud and payment credential theft.
    - It requires banks or any other digital payment companies that carry out financial transactions to verify and identify all their customers.

6. **The Digital Personal Data Protection Act 2023 (DPDP):**
    - On August 11, 2023, the Indian Central Government passed its long-awaited Digital Personal Data Protection Act (DPDP). The act borrows its broad definition of personal data from EU's General Data Regulation Regulation (GDPR) and aims to protect data principles and restrict the activities of data fiduciaries.

CONCLUSION:

Implementing regulations has its challenges which include the understanding of the ever-evolving nature of technology, balancing individual privacy, and ensuring cybersecurity measures. The existing regulations though have had some impacts, but much needs to be done to prevent cases of Potential of AI, Ransome attacks data breaches. Policymakers and industry actors should work together to find practical solutions. Its enactment could serve as a milestone toward achieving effective cybersecurity and online privacy regulations.

REFERENCE:

1. Emerging Cybersecurity Trends in India
2. Section 43A of the IT Act, 2000
3. Kyle Chin, 'Top Cybersecurity Regulations in India' (*UpGuard*, 18 January 2024<www.upguard.com/blog/cybersecurity-regulations-india> accessed 26 March 2024, 13:10
4. Jorge Bernal Bernabe https://www.riverpublishers.com/research_details.php?book_id=711 accessed 26 March 2024, 11:30
5. Tejas B https://thelegalquorum.com/online-privacy-and-cybersecurity-challenges-and-regulations/ accessed 26 March 2024, 12:40.