International Journal of Engineering &Technology, 7 (3.12) (2018) 191-194

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Data Privacy and Cyber Security in the Age of IoT and Data Analytics: Response of Law

Rashmi Salpekar

Dean and Professor of Law,
Vivekananda Law School, Vivekananda Institute of Professional Studies
**Corresponding Author E-mail: rashmisalpekar@gmail.com*

Abstract

IoT and Data Analytics are developing and adopted very fast. Utilities are deploying smart meters, smart lighting, etc. Even the water supply distribution agencies are deploying smart water schemes to reduce non-revenue water. Further, data analytics is done by loT of companies to provide targeted advertising and knowing user preferences. All this requires co
llecting user data to be effective.
There is an urgent need to define unambiguous laws, well defined dispute resolution that defines the consumer liability and service provider liability in light of court judgments to that effect. Further, a cyber security framework also needs to be defined and also a cyber security maturity model needs to be in place to rate the cyber security of a given agency and the steps needed to make cyber security better.
The paper intends to study national and international laws on cyber security including framework and maturity model and data privacy laws. It will then come up with concrete enforceable suggestions to make cyber security better. The suggestions will include laws, liability, framework and guidelines.

Keywords: *Cybersecurity, IT Act, maturity model, privacy, law.*

1. Introduction

The advent of Internet of Things (IoT) and Data Analytics (DA) have heralded the connected world in home and office premises. There are even connected and driverless cars. Then there are smart meters and smart grids. IoT and DA require collection of user information and preferences which is collected over internet. Though the data transmission is encrypted, yet there is a possibility that the system may be hacked or in best case attacked. Further, the agency collecting data may use it for purposes other than which it was authorised to use e.g. predicting if home is occupied or not at a given time by analysing water, gas and electricity readings. An electricity company may promote some energy efficient products if it finds that a home or office is using high amount of electricity. An attacker may bring down home or office or even connected trains and cars.
Therefore, need is to make laws stronger and unambiguous. There is also a need to make legally enforceable framework, regulations and guidelines. A cyber security framework needs to be defined to rate the cybersecurity of utilities, agencies, homes, etc. All this will go a long way to make IoT and DA safe and secure and provide a credible deterrence.
The first thing to look at is the existing laws, regulations, guidelines, framework and maturity models.

2. The Indian Scenario

2.1 IT Act 2008[ITACT2008]

2.1.1 The Definitions

The IT Act has some definitions
The Act says (definition (ha) in Chapter I - Preliminary) "Communication Device means Cell Phones, Personal Digital Assistance (Sic), or combination of both or any other device used to communicate, send or transmit any text, video, audio, or image".
As per definition (nb) in Chapter I - Preliminary, "Cyber Security means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction".
There are two more relevant definitions:
Definition (ze) "Secure System means computer hardware, software, and procedure that" -:
a) "are reasonably secure from unauthorized access and misuse"
b) "provide a reasonable level of reliability and correct operation"
c) "are reasonably suited to performing the intended functions and"
d) "adhere to generally accepted security procedures"

Definition (zf) "Security Procedure means the security procedure prescribed under section 16 by the Central Government";
The Act lists the jail term for cybercrimes. It also defines cyber terrorism and punishment for it. It has given definition for computer resource too as a protected system which has a bearing on Critical Information Infrastructure, either in a direct or indirect manner. It deals with Breach of confidentiality and privacy and

defines penalty for breach. It mentions modes or methods for encryption.
However, there are shortcomings in this act in relation to IoT. Firstly, it does not include IoT and DA. Secondly, the definition of "Secure system" uses "reasonable" imply there is ambiguity. The methods of encryption do not mention modes of encryption. There is not even reference to BIS or ISO or any other standardisation body which should have been done.

2.1.2 Right to Privacy

On 24 August 2017, The Supreme Court of India passed a judgment on the matter of privacy, [SCRIGHTTOPRIVACY]. The salient points were
1. "Point 3(C): Privacy is a constitutionally protected right which emerges primarily from the guarantee of life and personal liberty in Article 21 of the Constitution".
2. "Point 3(E): Privacy is the constitutional core of human dignity. Privacy has both a normative and descriptive function. At a normative level privacy sub-serves those eternal values upon which the guarantees of life, liberty and freedom are founded. At a descriptive level, privacy postulates a bundle of entitlements and interests which lie at the foundation of ordered liberty".
3. "Point 3(G): This Court has not embarked upon an exhaustive enumeration or a catalogue of entitlements or interests comprised in the right to privacy. The Constitution must evolve with the felt necessities of time to meet the challenges thrown up in a democratic order governed by the rule of law".
4. "Point 3(H): Under Article 21, privacy is not an absolute right. A law which encroaches upon privacy will have to withstand the touchstone of permissible restrictions on fundamental rights".
5. "Point 5: Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but from non-state actors as well. We commend to the Union Government the need to examine and put into place a robust regime for data protection".
Looking at last point, it implies that the Supreme Court of India found that no regime existed for data protection and there was a need for this regime.
The author opines here that the data collected by utilities et al. should follow the below tenets
1. Data should be collected on need to know basis i.e. collect data enough to optimise the functions.
2. Data should always be protected securely e.g. encrypted with backups to make data available
3. Data to be collected must be defined and person from whom data is collected be explained properly the data and its use.
4. Policies for data collection need to be unambiguous and well defined
5. DA on data should only be concerned with need and not what can be done e.g. data should not predict if family is at home or persons are in office at given day and time.

2.1.3 The Bodies

The following bodies have been formed
Indian Computer Emergency Response Team (CERT-IN) vide General Statutory Rule 20(E) dated 16th January 2014. This is under Department of Electronics and Information Technology and performs functions mentioned in Section 70B of IT Act namely cyber security incident monitoring including preventive monitoring, analysis and forensic audits of cyber security incidents, information security assurance and audits, awareness and technology exposition in area of cyber security, training and upgrade of technical knowhow for entities and scanning of cyberspace for threats, vulnerabilities, breaches and malicious activities. It consists of persons from different government departments and cyber security experts.
National Critical Information Infrastructure Protection centre (NCIIPC) General Statutory Rule 19(E) dated 16th January 2014. The functions are under section 70A of IT Act. It is under control of National Technical Research Organisation. It is assigned the task of protecting all critical national information infrastructure. It is concerned with vulnerabilities, threats and attacks to the critical national information infrastructure. It is also involved in funding of innovative technology for this cause.

2.1.4 Guidelines, Frameworks and Regulations

In 2013, the Indian government through its Ministry of Electronics and Information Technology (MEITY) announced a national cyber security guidelines called CYBERSEC which served as a comprehensive course of action with respect to strategies related to securing the cyberspace. The defined mission was released as
"To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation."
The bodies such as NCIIPC and CERT-IN were created under this policy.
MEITY also notified rules for certain on case by case basis like[1]
a) "Notification No.G.S.R 446(E) dated 27.4.16 regarding Electronic Signature or Electronic Authentication Technique and Procedure Rules, 2016"
b) "Notification No. S.O.1581(E) dated 26.4.16 regarding Authorisation of CERT-In to monitor and collect traffic data or information in any computer resources u/s 69B"
c) "Notification No.993(E) dated 11.12.2015 regarding declaration of UIDAI-CIDR critical information under section 70A of IT Act"
The author has also found RBI notification for Cyber Security Framework in Banks dated 2nd June 2016. In this, RBI mandated setting up of Security Operations Centre. Apart from this, to deal with major identified aspects like "Detection", "Response", "Recovery" and "Containment", a Cyber Crisis Management Plan needs to be put into place. It lists the Baseline Cyber Security and Resilience Requirements and Cyber incident reporting template also.
There is a mention of national encryption policy which was issued by Government of India but was withdrawn later after receiving objections.

3. Worldwide Scenario

3.1 Laws

Through the directive 2013/40/EU dated 12 August 2013, EU has published information on assault against information systems. It defines the term "information systems". It also defines legal persons, liabilities, offences and penalties. It also clarifies EU member state jurisdiction. It also clarifies monitoring and statistics. It mandates Europol and ENISA, to collect data on cybercrime and network and information security at Union level so as to get an all-inclusive understanding of the issue at hand and thus formulate a more efficient and effective response. UK has applied this directive and defined Computer Misuse Act 1990 which, keeping in tune with changing times, have been amended twice through the Police and Justice Act 2006 and later the Serious Crime Act 2015[2]. Likewise each EU member country has its own set of laws, based on this directive[3].

USA has "Cyber security Information Sharing Act (CISA)", "Cyber security Enhancement Act of 2014", "Federal Exchange Data Breach Notification Act of 2015", "National Cyber security Protection Advancement Act of 2015", among many that deal with specific sectors. Further, each state has its own cyber security laws.

At Central level, USA has "1996 Health Insurance Portability and Accountability Act (HIPAA)", "1999 Gramm-Leach-Bliley Act" and "2002 Homeland Security Act", which included the "Federal Information Security Management Act (FISMA)". These acts directed all central agencies, financial organisations and healthcare institutions to install such measures that protected their information systems and data.

3.2 Privacy

User Data Privacy is embedded at design stage of system itself i.e. it is "Privacy By Design". For example the "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 (Article 29)[EUPRIVACY]". Privacy By Design relates to the "Trilogy" of following applications: 1) "IT systems"; 2) "Accountable business practices"; and 3) "Physical design and networked infrastructure".

3.3 Guidelines, Framework and Regulations

NIST ("National Institute of Standards and Technology") has developed a cyber security framework and guidelines for general purpose.

For smart grid sector:

European Commission Mandate "M/490 (Smart grid mandate)" is the "Standardisation mandate to European Standardisation Organisations (ESOs)" in order to sustain "European Smart Grid Deployment" and approves "CEN, CENELEC and ETSI" as uniform bodies.

NIST has developed standards for Cybersecurity framework and Department of Homeland Security has developed Cybersecurity Maturity Model for smart grid sector[C2M2].

The European Union and USA have issued mandates authorising standardisation for example US has IEEE, ANSI, EIA and Europe has ETSI, CENELEC, CEN, etc. ITU, ISO, IEC are some international standardisation bodies.

3.4 Summary of Worldwide scenario

An exhaustive study of laws, rules, regulations, framework and guidelines is beyond the scope of this paper but the salient points are

1. The Laws are unambiguous and penalties, offences and liabilities are well defined.
2. The rules, regulations and framework are well laid with little or no scope for ambiguity while allowing for future extensions
3. Even sector specific extensions to laws, rules, regulations, framework and guidelines is laid out.
4. Bodies are mandated by laws, rules, regulations and framework and there is little or no overlap.

4. So, What needs to be done in India?

The above shows that India has started paying attention to cybersecurity. However, as a next step the following needs to be done.

1. IT Act should be amended to define "Security". "Reasonably secure" is not the way to go. Mandates to enforce international standards should be given in the IT Act so that the standardisation body can enforce the standards. The national security policy only names ISO 27001, ISO 27032-12 which are not the only standards. A standardisation mandate will help in identifying the standards required to be adhered to. It should be noted here that mandate may be divided into two parts: common for all sectors and sector specific. The common part may be provided by IT Act (directly or vide a mandate issued under IT Act). Sector specific mandate shall be issued by sector regulator or ministry for sector where sector regulator does not exist.
2. MEITY has said "As per the Order, no person shall manufacture or store for sale, import, sell or distribute goods which do not conform to the Indian Standard specified in the Order. Manufacturers of these products are required to apply for registration from Bureau of Indian Standards (BIS) after getting their product tested from BIS recognized labs." This order is for registration of products but there is no mention of or relation to cybersecurity compliance.
3. A Common Cybersecurity framework needs to be issued with customisation points unambiguously defined. The customisation points may be used by sectors to implement their own framework deviations as per the sector requirement. Further, MEITY has issued rules (both GSR and case by case rules). There should be unambiguous set of rules for cyber security included in this framework directly or referenced by this framework.
4. Common Cyber Security guidelines need to be issued with customisation points unambiguously defined. The customisation points may be used by sectors to implement their own guideline deviations as per the sector requirement.
5. It should be possible to amend the framework and guidelines as per further developments.
6. A Cyber Security Maturity Model should be developed to rate the cyber security of different organisations. This will help the organisations improve their cyber security to reach highest levels.
7. There should be no need to have a national encryption policy because encryption depends on algorithms which can be replaced. Further, each organisation should have freedom to choose encryption strength based on their security and data protection requirement.

References

[1] [ITACT2008] Ministry of Law, Justice and Company Affairs (Legislative Department): The Information Technology ACT, 2008

[2] MEITY website http://meity.gov.in/ (standards are in http://meity.gov.in/esdm/standards)

[3] [CYBERSEC] MEITY: National Cybersecurity Policy, 2013

[4] MEITY: G.S.R 19 (E) - Information Technology (National critical Information Infrastructure Protection centre and manner of performing function and duties) Rules, 2013 dated 16.01.2014

[5] MEITY: G.S.R 20 (E) -Information Technology(The Indian Computer emergency response team and manner of performing function and duties) Rules,2013 dated 16.01.2014

[6] BIS RULES: http://www.bis.org.in/bs/bisrules.htm

[7] CERT-IN: http://www.cert-in.org.in/

[8] [INFOATTACKS] The European Parliament and The Council of European Union: Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, dated 12 August 2013

[9] European Commission Directorate-General for Energy: M/490 Standardisation Mandate European Standardisation Organisations (ESOs) to support European Smart Grid deployment, Brussels 1st March 2011

[10] [EUPRIVACY] The Working Party on the Protection of Individuals With Regard To the Processing of Personal Data[4]: Article 29 Data Protection Working Party, Opinion 12/2011 on smart metering, Adopted on 4 April 2011

[11] [C2M2] U.S. Department of Homeland Security: Cybersecurity Capability Maturity Model (C2M2), Version 1.1 February 2014

[12] National Institute of Standards and Technology: Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0 February 12, 2014

[13] [SCPRIVACY] Supreme Court Of India: Justice K S Puttaswamy (Retd.), and anr. vs. Union of India and Ors. (Writ Petition (Civil) NO 494 OF 2012), dated 24th August 2017
[14] https://www.gracefulsecurity.com/uk-cyber-crime-law/
[15] https://blog.appknox.com/a-glance-at-the-united-states-cyber-security-laws/