UNIT- 5
LEGAL, ETHICAL AND PROFESSIONAL ISSUES IN INFORMATION SECURITY


information
security

INTRODUCTION

- _You must understand scope of an organization's legal and ethical responsibilities .
- To minimize liabilities/reduce risks, the information security practitioner must:

- Understand current legal environment
- Stay current with laws and regulations
- Watch for new issues that emerge

Copyright Infringement

Identity Theft

Click fraud

Hacking

LAWS AND ETHICS IN INFORMATION SECURITY

- LAWS- The rules the members of a society create to balance the individual rights to self-determination against the needs of the society as a whole.
- ETHICS- It is defined as socially acceptable behaviors.
- Laws are rules that mandate or prohibit certain behavior; they are drawn from ethics.
- The key difference between laws and ethics is that laws carry the authority of a governing body, and ethics do not.

LAWS AND ETHICS IN INFORMATION SECURITY

- Ethics in turn are based on cultural mores:

👇the fixed moral attitudes or customs of a particular group.

👇Some ethical standards are universal.

👇For example, murder, theft, assault, and arson are actions that deviate from ethical and legal codes throughout the world.

ORGANISATIONAL LIABILITY AND THE NE FOR COUNSEL

- What if an organization does not demand or even encourage strong ethical behavior from its employees?
- What if an organization does not behave ethically?

- Even if there is no breach of criminal law, there can still be liability.
- **Liability** is the legal obligation of an entity that extends beyond criminal or contract law;
- It includes the legal obligation to make restitution, or to compensate for wrongs committed

ORGANISATIONAL LIABILITY AND THE NE FOR COUNSEL

- The bottom line is that if an employee, acting with or without the authorization of the employer, performs an illegal or unethical act that causes some degree of harm, the employer can be held financially liable for that action.
- An organization increases its liability if it refuses to take measures known as due care.
- **Due care** standards are met

▲ when an organization makes sure that every employee knows what is acceptable or unacceptable behavior,

▲ knows the consequences of illegal or unethical actions.

ORGANISATIONAL LIABILITY AND THE NE
FOR COUNSEL

- **Due diligence** requires
  - an organization make a valid effort to protect others and continually maintains this level of effort.
- **Long arm jurisdiction**—
  - the long arm of the law extending across the country or around the world to draw an accused individual into its court systems.

POLICY VERSUS LAW

- Policies
  - Guidelines that describe acceptable and unacceptable employee behaviors.
  - Functions as organizational laws.
  - Has penalties, judicial practices, and sanctions.
- Difference between policy and law-
  - Ignorance of policy is acceptable.
  - Ignorance of law is unacceptable.

What Ethics can be Followed in IT?

- Never Piracy Online…
- Follow Up the Social Reputation…
- Never Harm the Public Websites…
- Closure of Digital Hacking…
- Certify Websites Who Deal with Payments…
- Never Do Fraudulent Activities…
- Never Give Misguided Information…
- Never Steal Information online for Reproduction…
- Never Create a False Evidence Using IT…
- Utilizing the IT in a Manner to Get Benefits Only…

WHAT IS CYBER CRIME?

CYBER CRIME

At the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, cybercrime was broken into two categories and defined as:

a. **Cybercrime in a narrow sense (computer crime**): Any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them.

b. Cybercrime in a broader sense (computer-related crime): Any illegal behavior committed by means of a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network.

CYBER CRIME

The OECD Recommendations of 1986 included a working definition as a basis for the study:

- Computer-related crime is considered as any illegal, unethical or unauthorized behaviour relating to the automatic processing and the transmission of data.

Cyber frauds in India

As per the report, at least 1,15,000 people fall prey to cyber fraud every day, while 80 per minute and more than one per second leading to a rise in the average direct financial cost per victim to around Rs10,500.

Types Of Cyber Crime

- Hacking
- Child Pornography
- Denial of Service Attack
- Virus Dissemination
- Computer Vandalism
- Cyber Terrorism
- Software Privacy

CYBER CRIMES FOUND IN INDIA

1. **Sale of illegal articles:** E.g. many of the auction sites even in India are believed to be selling cocaine in the name of ‘honey’.
2. **Online gambling:** Cases of hawala transactions and money laundering over the Internet have been reported. A man called Kola Mohan invented the story of winning the Euro Lottery. He himselfcreated a website and an email address on the Internet with the address 'eurolottery@usa.net.' Whenever accessed, the site would name him as the beneficiary of the 12.5 million pound. After confirmation a Telugu newspaper published this as a news. He collected huge sums from the public as well as from some banks for mobilization of the deposits in foreign currency. However, the fraud came to light when a cheque discounted by him with the Andhra Bank for Rs 1.73 million bounced. Mohan had pledged with Andhra Bank the copy of a bond certificate purportedly issued by Midland Bank, Sheffields, London stating that a term deposit of 12.5 million was held in his name.

CYBER CRIMES FOUND IN INDIA

4. **Intellectual Property crimes:** Yahoo had sued one Akash Arora for use of the domain name 'Yahooindia.Com' deceptively similar to its 'Yahoo.com'. As this case was governed by the Trade Marks Act, 1958, the additional defence taken against Yahoo's legal action for the interim order was that the Trade Marks Act was applicable only to goods.
5. **Email spoofing :** Example- An Executive's case, where he pretended to be a girl and cheated an Abu dhabi based NRI for crores by blackmailing tactics.
6. **Unauthorized access to computer systems or networks :** "Dr. Nuker", who claims to be the founder of Pakistan Hackerz Club, reportedly hacked the websites of the Indian Parliament, Ahmedabad Telephone Exchange, Engineering Export Promotion Council, and United Nations (India).

CYBER CRIMES FOUND IN INDIA

7. **Email bombing:** a foreigner who had been residing in Simla, India for almost thirty years wanted to avail of a scheme introduced by the Simla Housing Board to buy land at lower rates. When he made an application it was rejected on the grounds that the scheme was available only for citizens of India. He decided to take his revenge. Consequently he sent thousands of mails to the Simla Housing Board and repeatedly kept sending e-mails till their servers crashed.
8. **Salami attacks:** E.g. A bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 5 a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizeable amount of money every month.

CYBER CRIMES FOUND IN INDIA

- **9. Trojan Attack:** To cite an example, two friends Rahul and Mukesh (names changed), had a heated argument over one girl, Radha (name changed) whom they both liked. When the girl, asked to choose, chose Mukesh over Rahul, Rahul decided to get even. On the 14th of February, he sent Mukesh a spoofed e-card, which appeared to have come from Radha's mail account. The e-card actually contained a Trojan. As soon as Mukesh opened the card, the Trojan was installed on his computer. Rahul now had complete control over Mukesh's computer and proceeded to harass him thoroughly.

CYBER CRIMES FOUND IN INDIA

- **10. Cyber stalking:** The Oxford dictionary defines stalking as "pursuing stealthily". Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc..

- A **passive attack** is a network **attack** in which a system is monitored and sometimes scanned for open ports and vulnerabilities. The purpose is solely to gain information about the target and no data is changed on the target.
- An **active attack** is a network exploit in which a hacker attempts to make changes to data on the target or data en route to the target. Types of **active attacks**: In a masquerade **attack**, the intruder pretends to be a particular user of a system to gain access or to gain greater privileges than they are authorized for.

Security

Confidentiality

- Traffic analysis

PASSIVE ATTACK

Integrity

- Modification
- Masquerading
- Replaying
- Non Repudiation
- Phishing

A **masquerade attack** is an **attack** that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification.

ACTIVE ATTACK

Availability

- Dos
- DDos

Nonrepudiation is a method of guaranteeing message transmission between parties via digital signature and/or encryption.

Traffic analysis

- Security concept that prevents the unauthorized disclosure of communication parameters. The successful implementation of this concept hides source and destination IP addresses, message length, and frequency of communication from unauthorized parties.

Phishing

- Typically a victim receives a message that appears to have been sent by a known contact or organization. An attachment or links in the message may install malware on the user's device or direct them to a malicious website set up to trick them into divulging personal and financial information, such as passwords, account IDs or credit card details. Phishing is a homophone of fishing, which involves using lures to catch fish.

THREATS : An act is proposed to perform a negative response in future.

↓

VULNERABILITIES : Is a loophole which allows an attacker to enter ones system .

↓

ATTACKS : An act that had performed a negative response .

↓

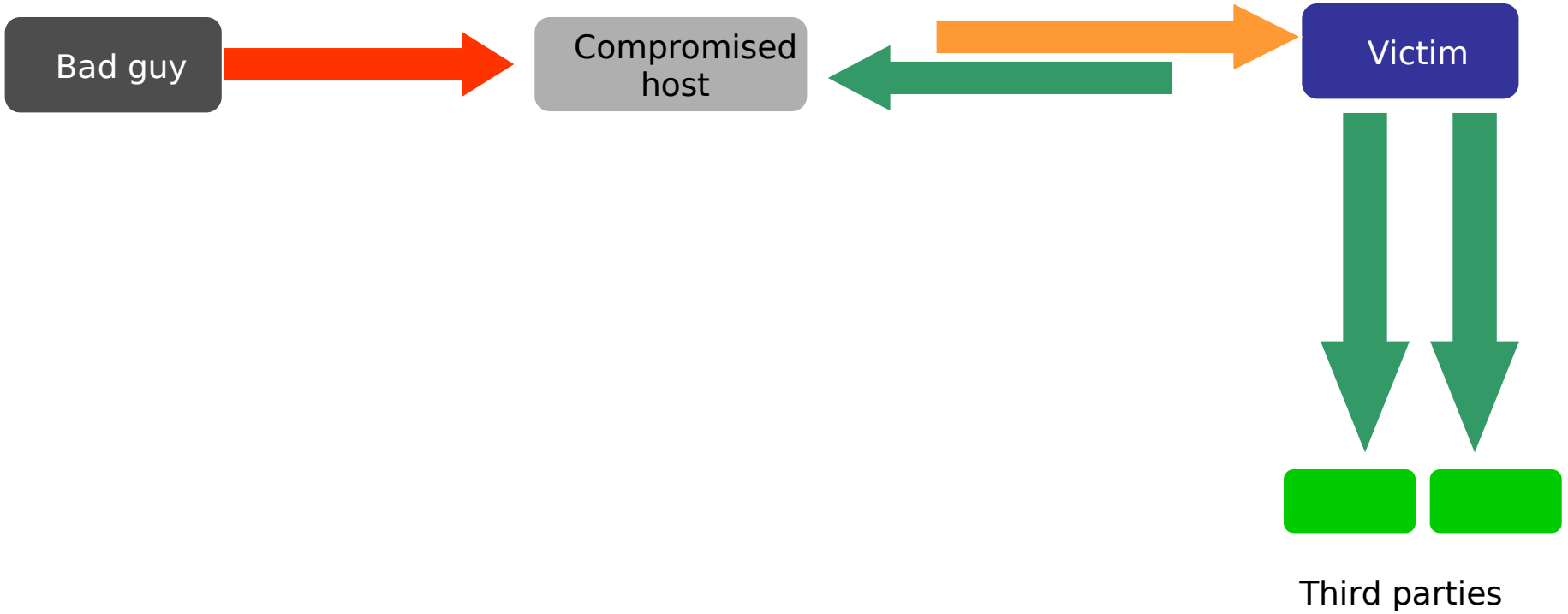
COUNTERMEASURES : Prevention of system from such negative responses.

What is denial of service attack?

- When a denial of service (DoS) attack occurs, a computer or a network user is unable to access resources like e-mail and the Internet. An attack can be directed at an operating system or at the network.

Denial of Service

DoS



What is distributed denial of service?

- A distributed denial of service (DDoS) attack is accomplished by using the Internet to break into computers and using them to attack a network. Hundreds or thousands of computer systems across the Internet can be turned into “zombies” and used to attack another system or website.

WHO COMMITS CYBER CRIME?

i. Insiders - Disgruntled employees and ex-employees, spouses, lovers

ii. Hackers - Crack into networks with malicious intent

iii. Virus Writers - Pose serious threats to networks and systems worldwide

iv. Foreign Intelligence - Use cyber tools as part of their Services for espionage activities and can pose the biggest threat to the security of another country

v. Terrorists - Use to formulate plans, to raise funds, propaganda

CYBER CRIME ON THE RISE

- As per the cyber crime data maintained by the National Crime Records Bureau (NCRB)

INFORMATION TECHNOLOGY ACT,2000	2007	2008	2009	2010
CASES FILED	217	288	420	966
ARRESTED	154	178	288	799

C YBER CRIME, INDIAN PENEL CODE (IPC)	2007	2008	2009	2010
CASES FILED	328	176	276	356
ARRESTED	429	195	263	294

CYBER CRIME ON THE RISE

- As per 2011 NCRB figures, there were 1791 cases registered under the IT Act during the year 2011 as compared to 966 cases during the previous year (2010) thereby reporting an increase of 85.4% in 2011 over 2010.
- Of this, 19.5% cases (349 out of 1791 cases) were reported from Andhra Pradesh followed by Maharashtra (306), Kerala (227), Karnataka (151) and Rajasthan (122). And 46.1% (826 cases) of the total 1791 cases registered under IT Act, 2000 were related to loss/damage to computer resource/utility reported under hacking with computer systems.
- According to NCRB, the police have recorded less than 5000; only 4829 cases and made fewer arrests (3187) between 2007-2011, under both the Information Technology (IT) Act as well as the Indian Penal Code (IPC).

CYBER CRIME ON THE RISE

- Out of total 157 cases relating to hacking under Sec. 66(2), most of the cases (23 cases) were reported from Karnataka followed by Kerala (22) and Andhra Pradesh (20 cases). And 20.4% of the 1184 persons arrested in cases relating to IT Act, 2000 were from Andhra Pradesh (242) followed by Maharashtra (226).
- The age-wise profile of persons arrested in cyber crime cases under the IT Act, 2000 showed that 58.6% of the offenders were in the age group 18–30 years (695 out of 1184) and 31.7% of the offenders were in the age group 30-45 years (376 out of 1184). Madhya Pradesh (10), Maharashtra (4), Kerala (3) and Delhi (2) reported offenders whose age was below 18years.

CYBER CRIME ON THE RISE

- Bangalore (117), Vishakhapatnam (107), Pune (83), Jaipur (76), Hyderabad (67) and Delhi (City) (50) have reported high incidence of cases (500 out of 858 cases) registered under IT Act, accounting for more than half of the cases (58.3%) reported under the IT Act.
- India has seen a total of 1.71 lakh cybercrimes in the past three-and-half-years and the number of crimes so far this year (27,482) indicate the total number is likely to cross 50,000 by December.
- At least one cybercrime was reported every 10 minutes in India in first six months of 2017. That's higher than a crime every 12 minutes in 2016.

CYBER CRIME ON THE RISE

WHAT KEEPS CYBER COPS ON TOES

Cyber Crime	2017 (till Oct)	2016
Online banking	2,095	1,343
FB-related	316	151
Email hacking	125	97
Sexual harassment	81	51
Lottery fraud	42	15
Data theft	47	43
Job fraud	49	40
Twitter-related	12	4
Total cases	**3,474**	**2,402**

CYBER LAW OF INDIA

- In India, cyber laws are contained in the Information Technology Act, 2000 ("IT Act") which came into force on October 17, 2000.
- The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government.
- The following Act, Rules and Regulations are covered under cyber laws:

1. Information Technology Act, 2000
2. Information Technology (Certifying Authorities) Rules, 2000
3. Information Technology (Security Procedure) Rules, 2004
4. Information Technology (Certifying Authority) Regulations, 2001

INFORMATION TECHNOLOGY ACTS

- *United Nations Model Law on Electronic Commerce 1996* (UNCITRAL Model)
- signed by President K. R. Narayanan on 9 May 2000. finalised by Pramod Mahajan

Section	Offence	Description	Penalty
66A	Publishing offensive, false or threatening information	Any person who sends by any means of a computer resource any information that is grossly offensive or has a menacing character; or any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult shall be punishable with imprisonment for a term which may extend to three years and with fine.	Imprisonment up to three years, with fine.

Continued

- Legal Recognition of Electronic Documents
- Legal Recognition of Digital Signatures
- Offenses and Contraventions
- Justice Dispensation Systems for cyber crimes.

Amendment Act 2008

- Focussing on data privacy
- Focussing on Information Security
- Defining cyber café
- Making digital signature technology neutral
- Defining reasonable security practices to be followed by corporate
- Redefining the role of intermediaries
- Recognising the role of Indian Computer Emergency Response Team
- Inclusion of some additional cyber crimes like cyber terrorism
- authorizing an Inspector to investigate cyber offences (as against the DSP earlier)

Sl.No	Offences	Section Under IT Act
1.	Tampering with computer source Documents	Sec.65
2.	Hacking with computer systems , Data Alteration	Sec.66
3.	Sending offensive messages through communication service, etc	Sec.66A
4.	Dishonestly receiving stolen computer resource or communication device	Sec.66B
5.	Identity theft	Sec.66C
6.	Cheating by personation by using computer resource	Sec.66D
7.	Violation of privacy	Sec.66E
8.	Cyber terrorism	Sec.66F
9.	Publishing or transmitting obscene material in electronic form	Sec .67
10.	Publishing or transmitting of material containing sexually explicit act, etc. in electronic form	Sec.67A
11.	Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form	Sec.67B
11.	Preservation and Retention of information by intermediaries	Sec.67C
12.	Powers to issue directions for interception or monitoring or decryption of any information through any computer resource	Sec.69
13.	Power to issue directions for blocking for public access of any information through any computer resource	Sec.69A
14.	Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security	Sec.69B
15.	Un-authorized access to protected system	Sec.70
16.	Penalty for misrepresentation	Sec.71
17.	Breach of confidentiality and privacy	Sec.72
18.	Publishing False digital signature certificates	Sec.73
19.	Publication for fraudulent purpose	Sec.74
29.	Act to apply for offence or contraventions committed outside India	Sec.75
21.	Compensation, penalties or confiscation not to interfere with other punishment	Sec.77
22.	Compounding of Offences	Sec.77A
23.	Offences with three years imprisonment to be cognizable	Sec.77B
24.	Exemption from liability of intermediary in certain cases	Sec.79
25.	Punishment for abetment of offences	Sec.84B
26.	Punishment for attempt to commit offences	Sec.84C
27.	Offences by Companies	Sec.85
	Note : Sec.78 of I.T. Act empowers Police Inspector to investigate cases falling under this Act	
28.	Sending threatening messages by e-mail	Sec .503 IPC
29.	Word, gesture or act intended to insult the modesty of a woman	Sec.509 IPC
30.	Sending defamatory messages by e-mail	Sec .499 IPC
31.	Bogus websites , Cyber Frauds	Sec .420 IPC
32.	E-mail Spoofing	Sec .463 IPC
33.	Making a false document	Sec.464 IPC
34.	Forgery for purpose of cheating	Sec.468 IPC
35.	Forgery for purpose of harming reputation	Sec.469 IPC

36.	Web-Jacking	Sec .383 IPC
37.	E-mail Abuse	Sec .500 IPC
38.	Punishment for criminal intimidation	Sec.506 IPC
39.	Criminal intimidation by an anonymous communication	Sec.507 IPC
40.	When copyright infringed:- Copyright in a work shall be deemed to be infringed	Sec.51
41.	Offence of infringement of copyright or other rights conferred by this Act. Any person who knowingly infringes or abets the infringement of	Sec.63
42.	Enhanced penalty on second and subsequent covictions	Sec.63A
43.	Knowing use of infringing copy of computer programme to be an offence	Sec.63B
44.	Obscenity	Sec. 292 IPC
45.	Printing etc. of grossly indecent or scurrilous matter or matter intended for blackmail	Sec.292A IPC
46.	Sale, etc., of obscene objects to young person	Sec .293 IPC
47.	Obscene acts and songs	Sec.294 IPC
48.	Theft of Computer Hardware	Sec. 378
49.	Punishment for theft	Sec.379
50.	Online Sale of Drugs	NDPS Act
51.	Online Sale of Arms	Arms Act

NEED FOR CYBER LAW IN INDIA

- Firstly, India has an extremely detailed and well-defined legal system in place. Numerous laws have been enacted and implemented and the foremost amongst them is The Constitution of India. However the arrival of Internet signalled the beginning of the rise of new and complex legal issues. It may be pertinent to mention that all the existing laws in place in India were enacted way back keeping in mind the relevant political, social, economic, and cultural scenario of that relevant time. Nobody then could really visualize about the Internet. Despite the brilliant acumen of our master draftsmen, the requirements of cyberspace could hardly ever be anticipated. As such, the coming of the Internet led to the emergence of numerous ticklish legal issues and problems which necessitated the enactment of Cyber laws.

NEED FOR CYBER LAW IN INDIA

- Secondly, the existing laws of India, could not be interpreted in the light of the emerging cyberspace, to include all aspects relating to different activities in cyberspace. In fact, the practical experience and the wisdom of judgment found that it shall not be without major perils and pitfalls, if the existing laws were to be interpreted in the scenario of emerging cyberspace, without enacting new cyber laws. Hence,the need for enactment of relevant cyber laws.

NEED FOR CYBER LAW IN INDIA

- Thirdly, none of the existing laws gave any legal validity or sanction to the activities in Cyberspace. For example, the Net is used by a large majority of users for email. Yet till today, email is not "legal" in our country. There is no law in the country, which gives legal validity, and sanction to email. Courts and judiciary in our country have been reluctant to grant judicial recognition to the legality of email in the absence of any specific law having been enacted by the Parliament. As such the need has arisen for Cyber law.

NEED FOR CYBER LAW IN INDIA

- Fourthly, Internet requires an enabling and supportive legal infrastructure in tune with the times. This legal infrastructure can only be given by the enactment of the relevant Cyber laws as the traditional laws have failed to grant the same. E-commerce, the biggest future of Internet, can only be possible if necessary legal infrastructure compliments the same to enable its vibrant growth.

NEED FOR CYBER LAW IN INDIA

- Almost all transactions in shares are in demit form.
- Almost all companies extensively depend upon their computer networks and keep their valuable data in electronic form.
- Government forms including income tax returns, company law forms etc. are now filled in electronic form.
- Consumers are increasingly using credit cards for shopping.
- Most people are using email, cell phones and SMS messages for communication.

- Even in "non-cyber crime" cases, important evidence is found in computers / cell phones e.g. in cases of divorce, murder, kidnapping, tax evasion, organized crime, terrorist operations, counterfeit currency etc.
- Cyber crime cases such as online banking frauds, online share trading fraud, source code theft, credit card fraud, tax evasion, virus attacks, cyber sabotage, phishing attacks, email hijacking, denial of service, hacking, pornography etc are becoming common.
- Digital signatures and e-contracts are fast replacing conventional methods of transacting business

CASE LAWS

- **Avnish Bajaj Vs. State (N.C.T.) of Delhi**
- Avnish Bajaj – CEO of Baazee.com, a customer-to-customer website, which facilitates the online sale of property. Baazee.com receives commission from such sales and also generates revenue from advertisements carried on its web pages. An obscene MMS clipping was listed for sale on Baazee.com on 27th November, 2004 in the name of "DPS Girl having fun". Some copies of the clipping were sold through Baazee.com and the seller received the money for the sale. Avnish Bajaj was arrested under section 67 of the Information Technology Act, 2000. The arguments of the defendant were that - Section 67 of the Information Technology Act relates to publication of obscene material. It does not relate to transmission of such material. On coming to learn of the illegal character of the sale, remedial steps were taken within 38 hours, since the intervening period was a weekend.

CASE LAWS

The findings of the Court –

- It has not been established from the evidence that any publication took place by the accused, directly or indirectly.
- The actual obscene recording/clip could not be viewed on the portal of Baazee.com.
- The sale consideration was not routed through the accused.
- Prima facie Baazee.com had endeavored to plug the loophole.
- The accused had actively participated in the investigations.
- The nature of the alleged offence is such that the evidence has already crystallized and may even be tamper proof.
- Even though the accused is a foreign citizen, he is of Indian origin with family roots in India.

CASE LAWS

- The evidence that has been collected indicates only that the obscene material may have been unwittingly offered for sale on the website.
- The evidence that has been collected indicates that the heinous nature of the alleged crime may be attributable to some other person.
- The court granted bail to Mr. Bajaj subject to furnishing two sureties of Rs. 1 lakh each. The court ordered Mr. Bajaj to surrender his passport and not to leave India without the permission of the Court. The court also ordered Mr.Bajaj to participate and assist in the investigation.

INTELLECTUAL PROPERTY

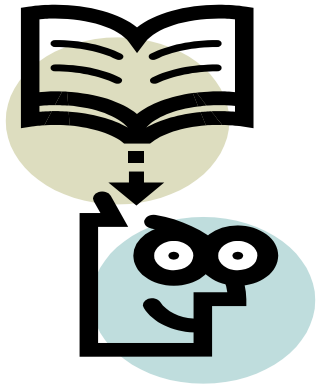
The term ‘intellectual property’ (IP) refers to property created with the use of human intellect.

IP refers to all creations of mind which are vested with the status of property because of the commercial valu associated with the intellectual creation. i.e. inventions in all fields of human endeavor, scientific discoveries, industrial designs for article, literary & artistic work, symbols etc. used in commerce.

Nature/ characteristics of Intellectual Property:

- Creation of human mind (Intellect)
- Intangible property
- Exclusive rights given by statutes
- Time-bound and Territorial/Jurisdictional

What is Intellectual Property Right (IPR)?



Intellectual Property Right

- not to be confused with IP
- it is a right vested in the asset, not the asset itself
- e.g.
  - an idea / invention is IP, a patent registration is an IPR
  - a customer / price list is IP, a right of confidentiality is an IPR
  - a secret production method is IP, a right to a trade secret is an IPR
  - a particular way of representation is IP, copyright or a design registration is an IPR
  - a brand / trade name is IP, a trade mark registration is an IPR

Intellectual property in India

INDUSTRIAL PROPERTY + COPY RIGHT

PATENTS

DESIGNS

TRADEMARKS

Geographical Indications

Patents & Designs

Patent Information

Trade Marks

Copy Right

Geographical Indications

INDUSTRIAL PROPERTY

Patents	Designs	Trade- Marks	Geographical Indications
Inventions relating to constructional features	any modification in shape,pattern, configuration	Word Name Logo	Indications of source origin or geography
e.g. Safety Valve, Mechanism of a PRESSURE COOKER	e.g. shape of a handle or body portion of a pressure cooker	e.g. for same Pressure Cooker “PRESTIGE” “HAWKINS” “MAHARAJA”	Darjeeling tea Kanchipuram sarees Kolhapurl chappals

‘Trade Mark’ – Definition under the Trade Marks A

Trade mark means, a mark capable of being represented graphically and which is capa
distinguishing the goods or services of one person from those of others and may inclu
goods, their packaging and combination of colures....

"mark" includes a **device, brand, heading, label, ticket, name, signature, word, letter, numeral, shape of goods, packaging or combination of colours** or **any combination thereof**;

[S. 2 (1) (zb) Trade Marks Act 1999]

JUST DO IT.

Notice of Registration

®

TM

_____ is a trademark/service mark of _____

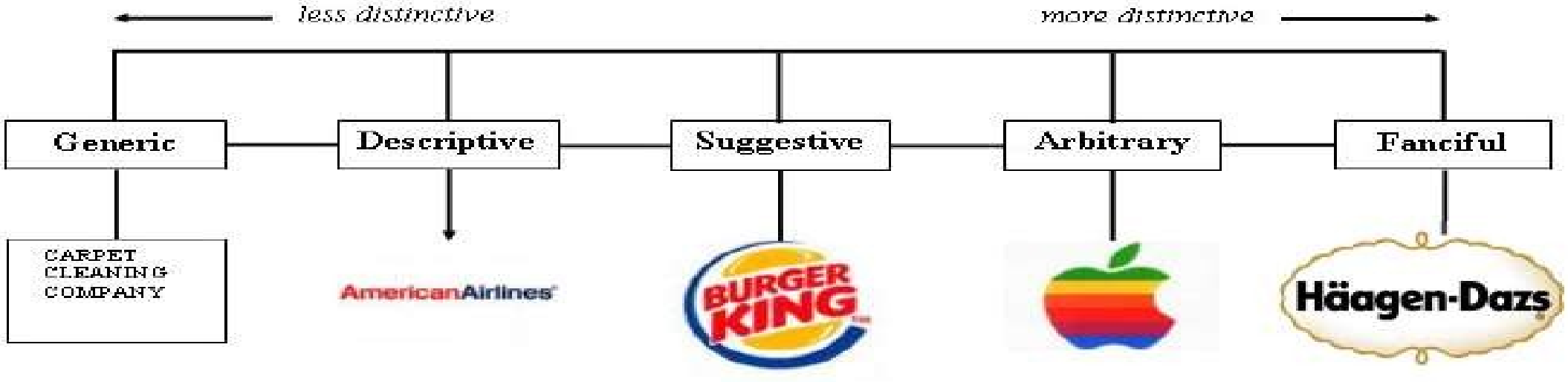
SM

Purpose & functions of a Trademark

- To identify the origin of the product/service.
- To distinguish the product/service of the proprietor from those
- To guarantee the quality of the product/service, and
- To advertise the product/service.

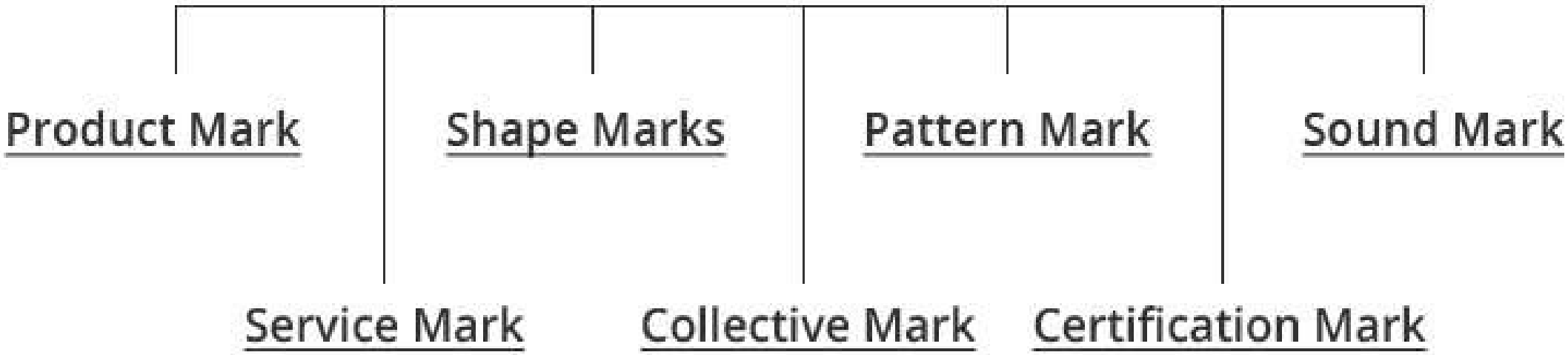
Selecting a Mark

Distinctiveness Spectrum



The more distinctive the mark, the greater its level of legal protectability. Generic marks are not capable of trademark protection. Descriptive marks are capable of protection only with a showing of secondary meaning.

TYPES OF TRADEMARK IN INDIA



Product Mark

- A product mark is similar to trademark only, but it is to identify the products or goods instead of services. Herein the product is the unique selling feature of the company. Initially, TM, which states that the mark is not yet registered. Once they are registered, they have to use ® .
- **Examples:** Pepsi® , Maggi® , PHILIPS® etc.

Service Mark

- This type of trademark is used to identify and distinguish the services rather than the products.
- Like intangible products , transport, communication or other utilities such as electricity, water, routine maintenance or repair work, etc.
- The Service marks have their particular symbol which is SM and not TM.

A very prominent **example** is McDonald's, which is a service mark for restaurant services.

Collective Mark

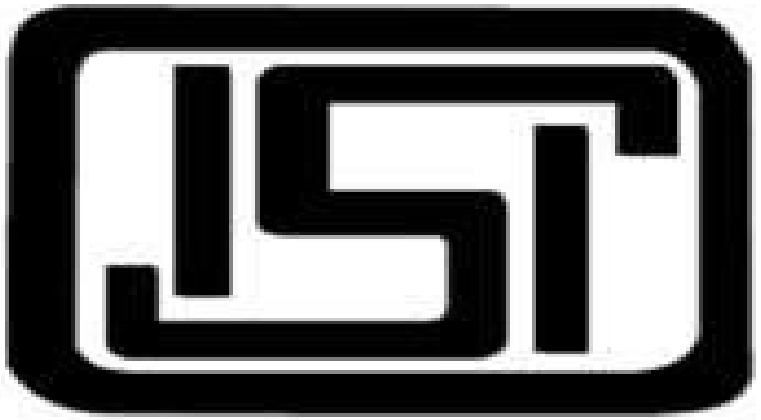
A **collective mark** is owned by a collective, whose members use the collective mark to identify their goods and services and to distinguish their goods and services from those of non-members, and to indicate membership in the group.

- **Examples** are like "CA" device is used by the members who fall under Institute of Chartered Accountants; another example is "CPA" which denotes members of the Society of Certified Public Accountants.

Certification marks

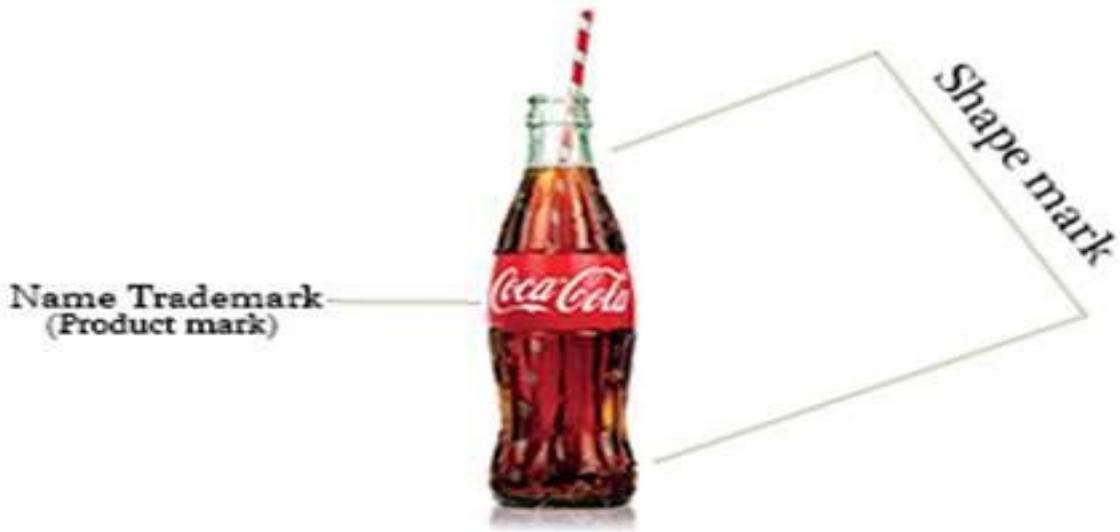
Certification marks are used to define "standard" of goods and services.

Example: Woolmark, which is certified for the fabrics on clothing, Agmark, and ISI.



Shape Marks

To sum up shape trademarks, it has facilitated promotion of products and emerged into the trademark type after the technological advancement of graphics and other forms of animation technology. The graphical representation which is able to make a difference amongst the products can be shape marked. An example can be the Galliano liquor bottle.

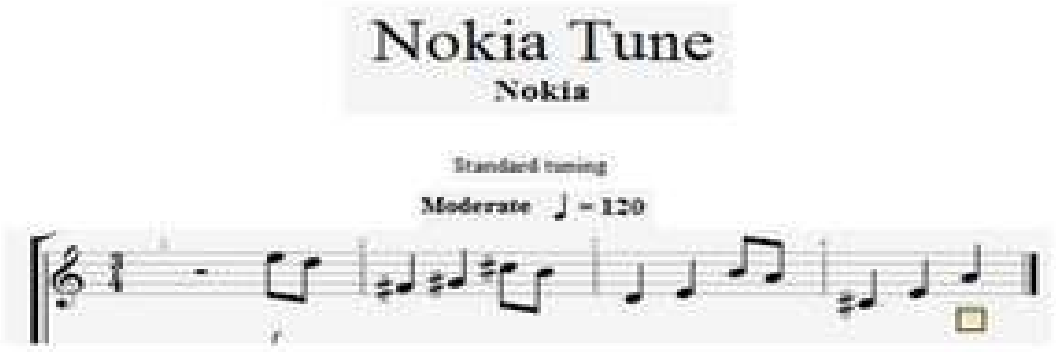


Pattern Mark

- The general meaning of pattern is a repetition of similar design, so it is a type of trademark wherein the pattern is able to distinguish the product and services of one brand from another. These are difficult to be distinguished and have high chances of infringement with near similar designs.
- They at times, fail to make a distinction and the registration would not be accepted unless they have evidence of distinctiveness.

Sound Mark

- The sound graphics that distinguish the products and services of one from the other.
- The sound logo can comprise musical notes, words and sound graphics. The first Sound Mark to be registered in India was Yahoo yodel followed by Nokia tune.



Loss of Rights

- Improper use
- Genericide
- Non-use
- Improper assignment or licensing
- Failure to police
- Failure to renew
- Cancellation

Benefits of Registration of a trademark

- **Registration is prima facie evidence of proprietorship of the trademark**
- **It gives the exclusive right to use the trademark in respect of goods/services; and to take legal action in case of infringement**
- **The registered proprietor may assign or license the trademark as any other property**
- **The registered proprietor can enjoy the Goodwill associated with registered trademark forever, if the mark is renewed from time to time**

Steps for registration of trademark in India

- **Select a good trademark**
- **Apply for registration on appropriate form with appropriate fee**
- **Classify your goods & services and specify them properly**
- **Apply before appropriate office of the Trade Marks Registry; and**
- **Respond to office queries/notices properly and on time**

Selecting a good Trademark

Go for a trademark which is-

- *Easy to speak & spell* (in case of word mark),
- *Appealing and easy to remember or recollect*.
- *invented or coined* word, unique monogram, logo or a geometrical device

Don't go for a trademark -

- *Which is not capable of distinguishing your goods or services* from those of others- like c
  letters or numerals, common surnames, words, pictures of the product concerned, etc.
  ……*Section 9(1)(a)]
- *Which refers to character or quality of goods/services* concerned, which indicate geogra
  which are common to trade, ….[Section 9(1) (b) & (c)]
- a deceptive, scandalous or offensive matter or a matter prohibited by law to be used as
  trademark……*Sections 9(2)(3) & 13]
- a mark which is same/similar to an already existing trademark ……*Section 11]

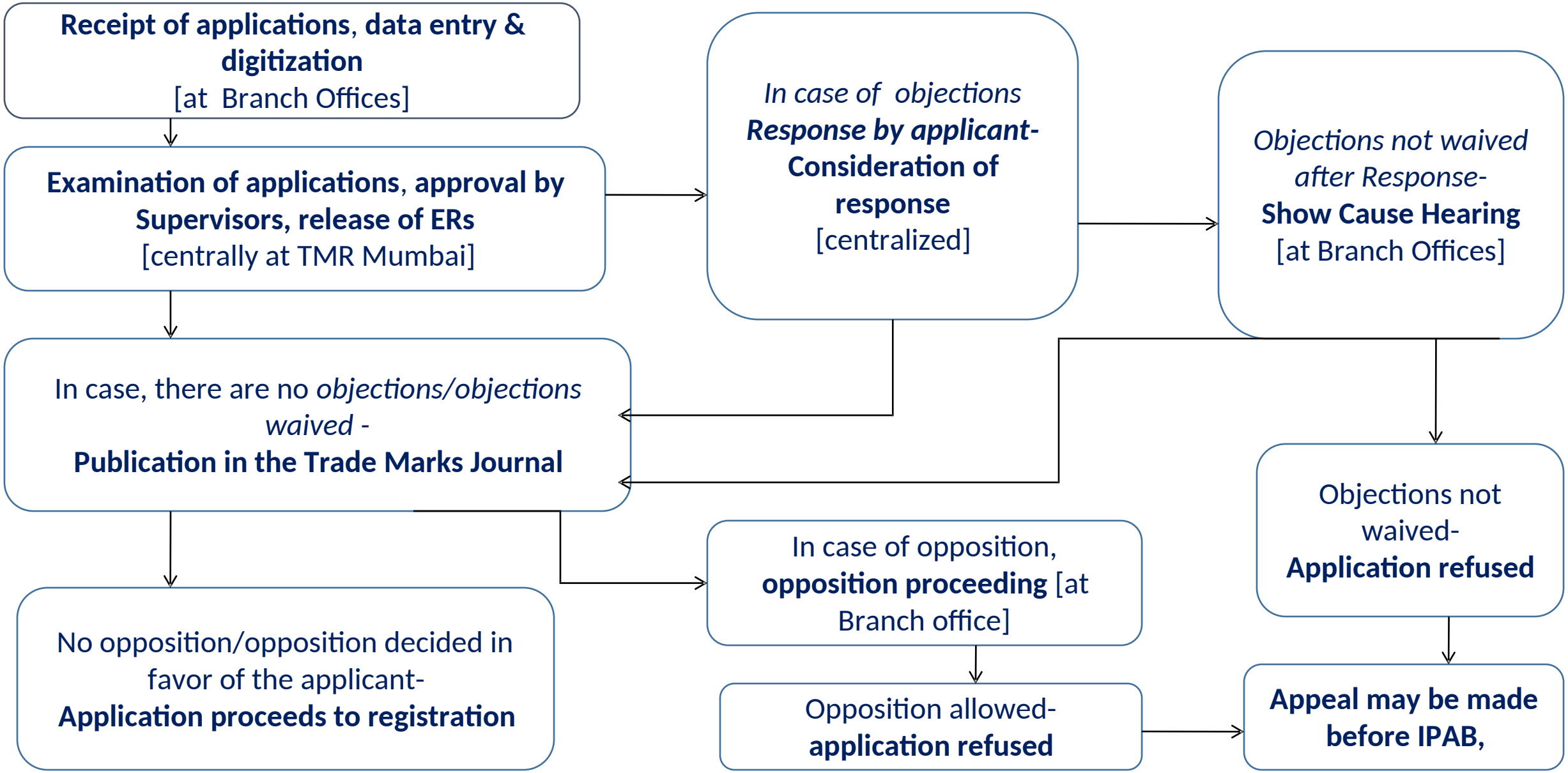
Appropriate form and fee

At present there are many forms prescribed for filing new applications depending on the nature of application such as Form TM-1, TM-2, TM-51, TM-52 TM-3, TM-8 etc.

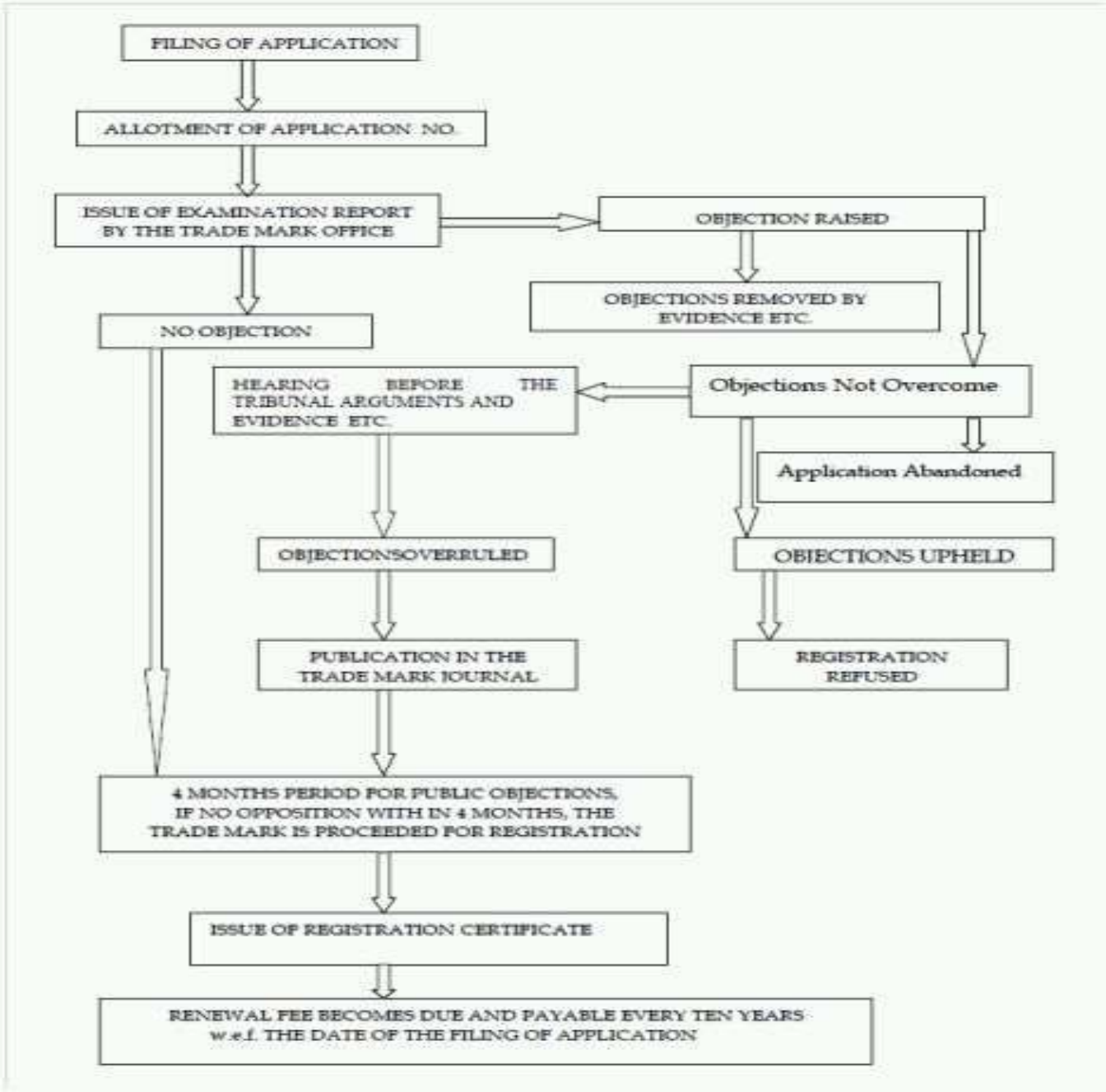
Fee ordinarily Rs.4000/-per class

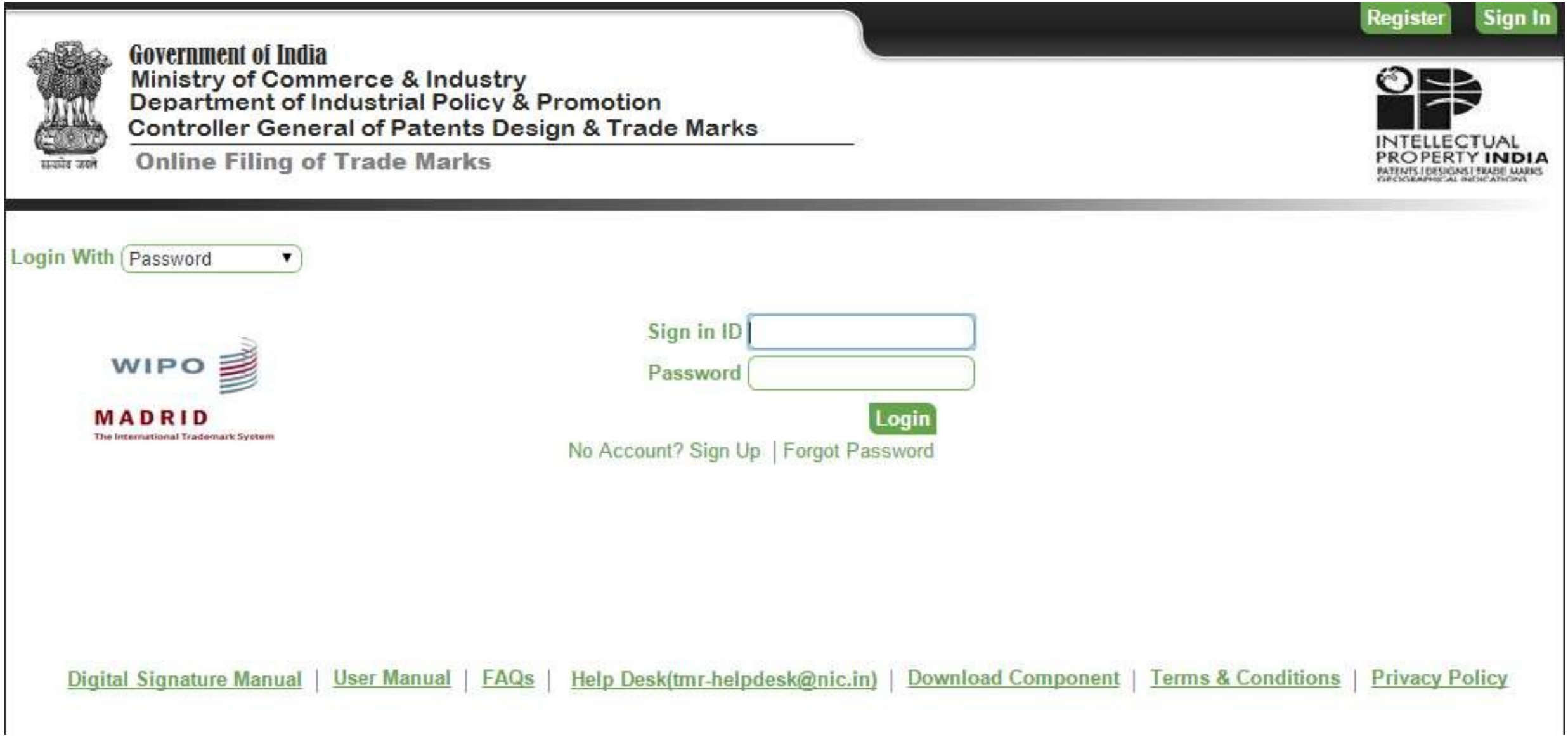
[In the proposed revised rules there will be only one form for all types of applications for registration of trademarks.]

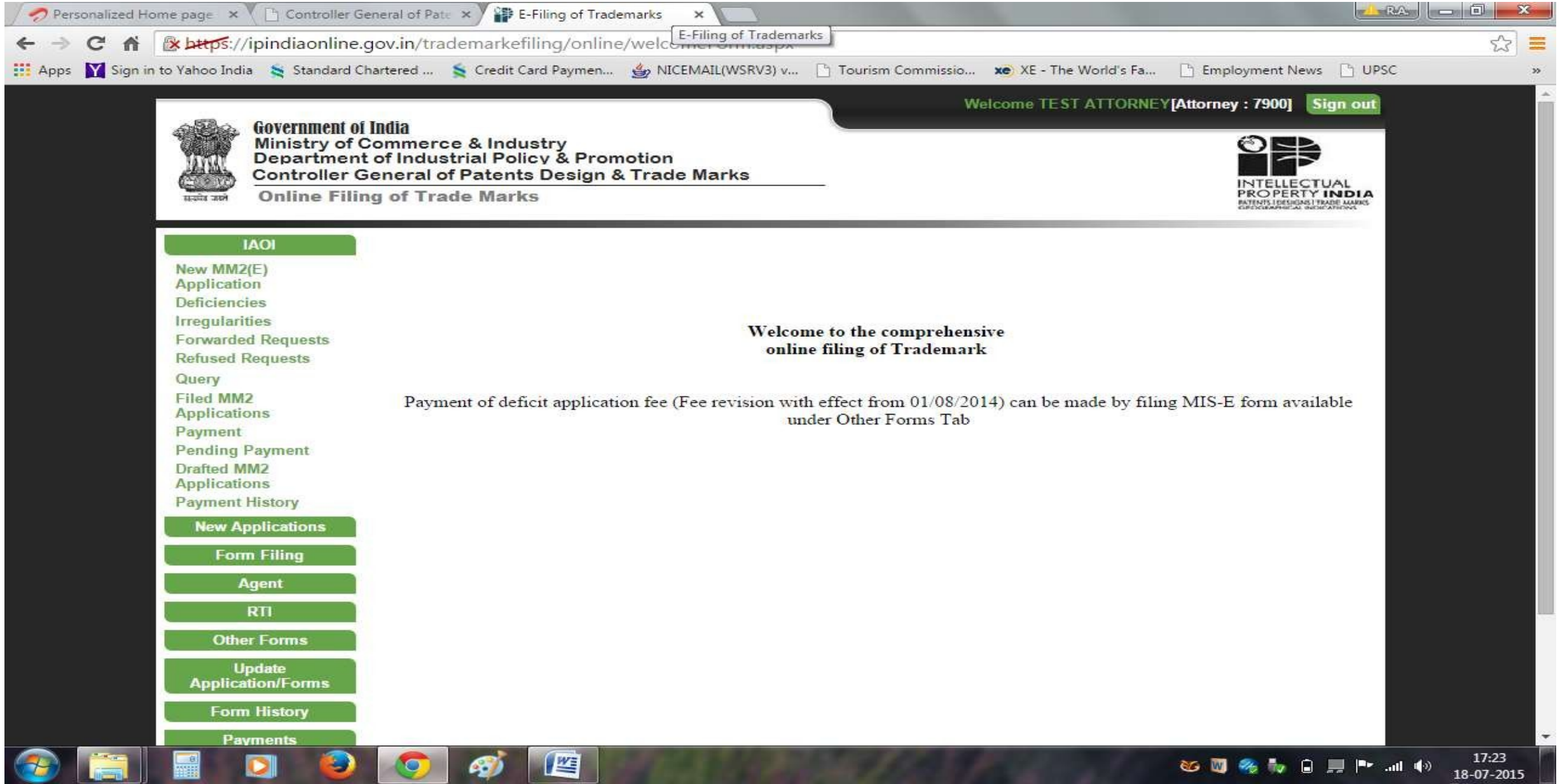
Steps involved in registration process

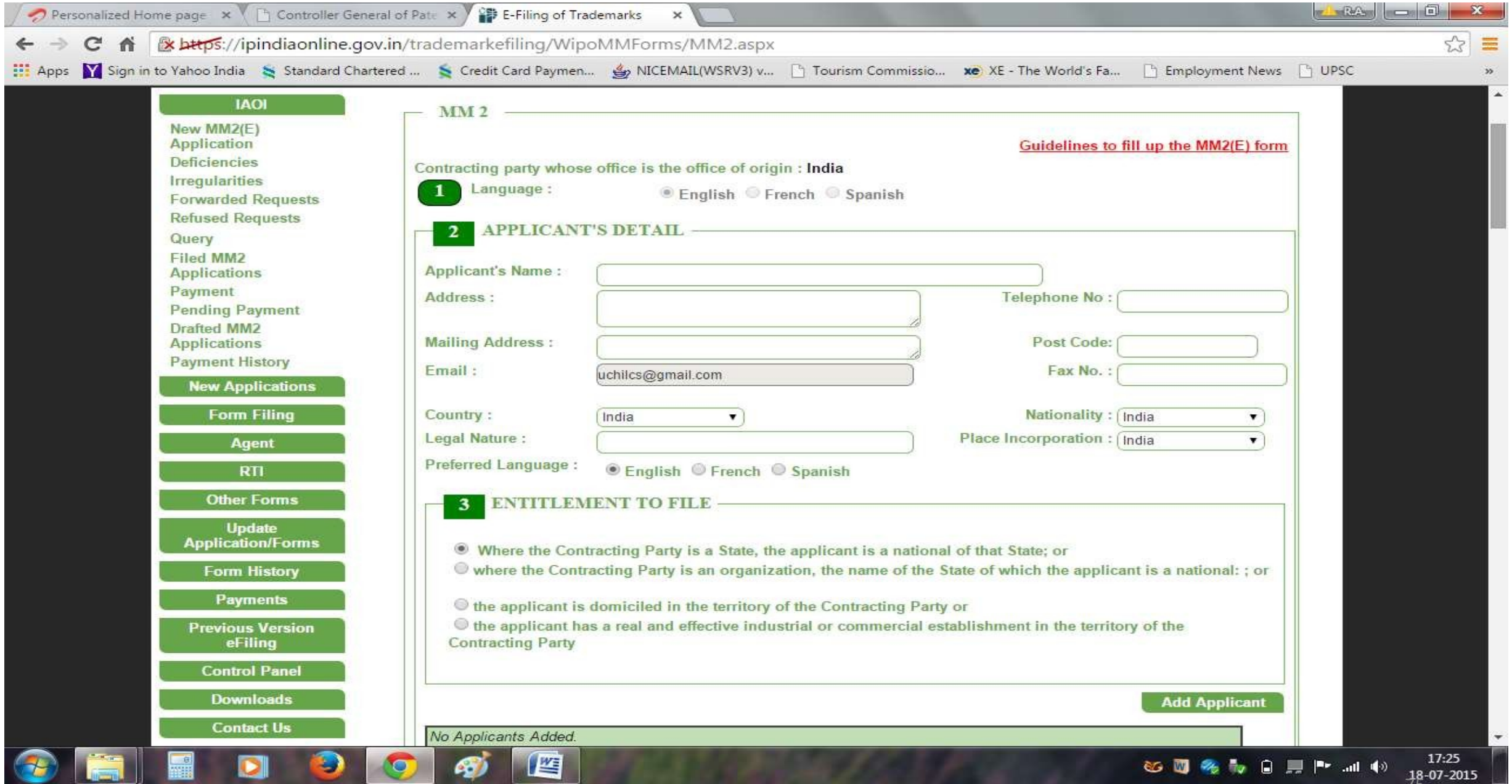


Steps involved in registration process




Register
Sign In
Government of India
Ministry of Commerce & Industry
Department of Industrial Policy & Promotion
Controller General of Patents Design & Trade Marks
Online Filing of Trade Marks
INTELLECTUAL PROPERTY INDIA
Login With
Password
WIPO
MADRID
The International Trademark System
Sign in ID
Password
Login
No Account? Sign Up | Forgot Password
Digital Signature Manual | User Manual | FAQs | Help Desk(tmr-helpdesk@nic.in) | Download Component | Terms & Conditions | Privacy Policy


Personalized Home page
Controller General of Pate
E-Filing of Trademarks
E-Filing of Trademarks
https://ipindiaonline.gov.in/trademarkefiling/online/welcomeformus.aspx
Apps
Sign in to Yahoo India
Standard Chartered ...
Credit Card Paymen...
NICEMAIL(WSRV3) v...
Tourism Commissio...
XE - The World's Fa...
Employment News
UPSC
Welcome TEST ATTORNEY[Attorney : 7900]
Sign out
Government of India
Ministry of Commerce & Industry
Department of Industrial Policy & Promotion
Controller General of Patents Design & Trade Marks
Online Filing of Trade Marks
INTELLECTUAL PROPERTY INDIA
IAOI
New MM2(E) Application
Deficiencies
Irregularities
Forwarded Requests
Refused Requests
Query
Filed MM2 Applications
Payment
Pending Payment
Drafted MM2 Applications
Payment History
New Applications
Form Filing
Agent
RTI
Other Forms
Update Application/Forms
Form History
Payments
Welcome to the comprehensive online filing of Trademark
Payment of deficit application fee (Fee revision with effect from 01/08/2014) can be made by filing MIS-E form available under Other Forms Tab
17:23
18-07-2015


Personalized Home page
Controller General of Pate
E-Filing of Trademarks
https://ipindiaonline.gov.in/trademarkefiling/WipoMMForms/MM2.aspx
Apps
Sign in to Yahoo India
Standard Chartered ...
Credit Card Paymen...
NICEMAIL(WSRV3) v...
Tourism Commissio...
XE - The World's Fa...
Employment News
UPSC
IAOI
New MM2(E) Application
Deficiencies
Irregularities
Forwarded Requests
Refused Requests
Query
Filed MM2 Applications
Payment
Pending Payment
Drafted MM2 Applications
Payment History
New Applications
Form Filing
Agent
RTI
Other Forms
Update Application/Forms
Form History
Payments
Previous Version eFiling
Control Panel
Downloads
Contact Us
MM 2
Guidelines to fill up the MM2(E) form
Contracting party whose office is the office of origin : India
1 Language : English French Spanish
2 APPLICANT'S DETAIL
Applicant's Name :
Address :
Telephone No :
Mailing Address :
Post Code:
Email : uchilcs@gmail.com
Fax No. :
Country : India
Nationality : India
Legal Nature :
Place Incorporation : India
Preferred Language : English French Spanish
3 ENTITLEMENT TO FILE
Where the Contracting Party is a State, the applicant is a national of that State; or
where the Contracting Party is an organization, the name of the State of which the applicant is a national: ; or
the applicant is domiciled in the territory of the Contracting Party or
the applicant has a real and effective industrial or commercial establishment in the territory of the Contracting Party
Add Applicant
No Applicants Added.
17:25
18-07-2015