Since the IT Act is one of the first attempts by the government at framing laws relating to cyberspace, it is evident that the wording of the law may end up giving law enforcement authorities a lot of powers that can be exercised at discretion.

Law enforcement officers who may not have been exposed to the internet or the culture of free speech that pervades cyberspace can be heavy-handed in their interpretation of the law. This has indeed been the case with a number of officers applying the law in a manner that has led to the arrest of private citizens. It has made sections of the public believe that the government is out to curb free speech and regulate our activities on the internet.

It thus becomes necessary to know which of our actions constitutes an offence under the IT Act.

**Q. The internet has no boundaries. Where does the reach of the IT Act extend to?**

The IT Act can be used to prosecute any offence committed by any person irrespective of nationality as long as the act or conduct that constitutes the offence or contravention involves a computer, computer system or network located in India.

Though the IT Act confers very wide ranging powers on the government, it recognizes the borderless nature of the internet and the fact that online services we often take for granted may be housed in any part of the world and be provided from any other part. Take, for instance, Gmail. Google, a company registered in the USA owns the service which is used by millions of people across the world to access their emails and other data that may be housed in servers located at different locations across the world.

Now imagine that an offensive email has caused you offence. Whose laws are applicable? Is it Indian laws because you are an Indian citizen, US laws because the company whose services you use is American or the laws of the country where the data was housed? These are troubling questions that have already had consequences because what constitutes an offence in one country may not necessarily be one in another.

**Q. What actions are offences under the IT Act?**

The following activities are termed offences under the IT Act. The punishments prescribed are also given. In all cases the punishments must be read as imprisonment upto ‘x’ years or fine or both:

|  |  |  |
| --- | --- | --- |
| **Offence** | **Max. prison** | **Max. Fine** |
| Tampering (destroying, altering or concealing) source code when it is to be maintained by law | 3 years | Rs 2 Lakh |
| Accessing without permission, downloading,introducing viruses, damaging or disrupting, denying access to or causing wrongful loss of personal or private information from a computer or computer network | 3 years | Rs 5 lakh |
| Sending information that is offensive, menacing, false but causes annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, misleading | 3 years | Not specified |
| Retaining a stolen computer or communication device | 3 years | Rs 1 Lakh |
| Making fraudulent or dishonest use of the electronic signature | 3 years | Rs 1 lakh |
| Publishing or transmitting the image of a private area of a person without his or her consent violating his/her privacy | 3 years | Rs 2 lakh |
| Wrongful loss or gain caused to a person because of negligent security practices and procedures in dealing with or handling sensitive personal data |  | Damages to person affected |
| Breaking a rule for which no penalty has been provided |  | Rs 25, 000 |

These are only some offences listed under the IT Act. There are other, more serious crimes like those of cyber terrorism which are covered later within this section.

**Q. What is Section 66A of the IT Act about?**

Section 66A gives broad powers to law enforcement agencies for prosecuting people based on any content they put up online, either through status messages or forum posts or blog entries. In brief, the following content or information can result in an offence:

- Information that is grossly offensive or has menacing character

- Information known to be false which causes annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will

- E-mail that causes annoyance or inconvenience or deceives the addressee or recipient about the origin of the message

These are very broad definitions and this section has often been used by zealous law enforcement officers to bring charges against people who believed they were exercising their right to free speech.

**Q. Who can investigate offences committed under the IT Act?**

All offences must be investigated by a police officer not below the rank of Inspector.

After a spate of incidents involving the arrest of laypersons that conveyed the impression that the government was stifling free speech, the central government issued guidelines that made it mandatory for a police official not below the deputy commissioner of police (DCP) to approve registration of complaints made under the controversial section 66(A).

Complaints under Section 66A can now be registered after approval of an officer of a rank not less than:

- DCP in urban and rural areas

- Inspector General (IG) in metros

**Q. What are the rules regarding pornography?**

The IT Act has several detailed provisions on pornography which can be seen in this page. [link to porno page]

**Q. What is cyber-terrorism?**

The IT Act defines cyber-terrorism as an act that:

- threatens the unity, integrity, security or sovereignty of India or strikes terror in the people.

- causes death or injury to people or damages property

- obtain through illegal access to a computer resource restricted information that is necessary to the security of the State or foreign relations

It can be caused by:

- denying or causing access to a computer resource to be denied to an authorized person.

- attempting to access a computer resource without authorization

- accessing a computer resource to which one does not have access to and obtains information that harms the sovereignty of the State or its relations with other nations

**Q. What is the punishment for cyber terrorism and who can investigate such a case?**

The investigating officer must be of the rank of an inspector.

Maximum punishment is life imprisonment.

**Q. What powers does a police officer have to arrest without warrant?**

Only a police officer of at least the rank of an inspector can enter a public place and search and arrest without a warrant.

If a person is arrested without a warrant by a person other than a police officer, the accused would have to be brought before a magistrate with jurisdiction in the case or before the officer-in-charge of a police station.

**Q. Who has the power to adjudicate on offences under this Act?**

An officer not below the rank of Director to the government of India or an equivalent officer of a State government can inquire into offences under this Act where the claim for injury or damages does not exceed Rs five crore.

The adjudicating officer has the power of a civil court.

**Q. Which offences are cognizable and which are not?**

Under the IT Act, offences which are punishable with imprisonment of three years and above are cognizable and those punishable with imprisonment of three years are bailable.

**Q. Can any of the offences committed under this Act be compounded?**

Compounding an offence refers to a settlement where both parties agree to a settlement on payment of cash. The IT Act disallows offences from being compounded in the following cases:

- When the punishment for the offence is life or imprisonment exceeding three years.

- When the accused is liable to enhanced punishment

- When the offence has been committed against a child (less than 18 years of age)

- When the offence affects the socio-economic conditions of the country

**Q. What documents does the IT Act no apply to?**

It does not apply to the following documents:

- A negotiable instrument (other than a cheque)

- A power-of-attorney

- A trust

- A will

- Any contract for the sale or conveyance of immovable property or any interest in such property.

--Ends