CONTENTIOUS SOFTWARE PIRACY VIA ILLEGALLY TRACKING

BY: MS. HARINDER NARVAN & MS. APARNA JAIN, KNOWLEDGENTIA CONSULTANTS

INTRODUCTION

Over the past decade, with the rise in numbers of users, the internet has been rampantly used as well as misused by the public at large. The tools which had been generated for the ease of connecting, doing business, communication, etc. are now the foundation for the perpetration of a range of 'cyber crimes' — from extortion to defamation to financial fraud, software piracy.

Law enforcement authorities in India have not exactly lagged behind in bringing these new age cyber criminals to task and have installed special 'Cyber crime cells' in different cities to combat crimes on the internet. These cells have been particularly adept at using IP Addresses information to trace individuals responsible for crimes. Very briefly, an Internet Protocol address (IP address) is a numeric label – a set of four numbers (Ex. 202.54.30.1) - that is assigned to every device (e.g., computer, printer) participating on the internet. Website operators and Internet Service Providers (ISP's) typically maintain data logs that track the online activity of each IP address that accesses their services. Although IP Addresses refer to particular computers – not necessarily individual users – it is possible to trace these addresses backwards to expose the individual behind the computer.

Information embedded in particular IP address-

When users visit a website, IP address will be available to that site. It is common for websites to keep a record of all IP addresses that visited with the data and time of the visit, even if this record is never used. ISP also has a record of user internet activity. Even if user IP address is a dynamic address – i.e. it changes every time user connect to the internet – an ISP will be able to identify user browsing activity because it knows what number was allocated to which customer and when.

Limited information is freely available about any IP address. Because IP addresses are allocated in batches. IP address can be static or dynamic. It will be in a particular range that typically reveals user choice of ISP and geographic location – though at best this will identify a city, not a street. Further it won't always identify the right city or even the right country, depending on user ISP and its system for allocating IP addresses.

Lawful disclosure of IP addresses-

Four sources are their under Indian law -

1. ISPs are required, under the operating license they are issued under the Telegraph Act, to provide assistance to law enforcement authorities.
2. Information Technology Act contains provisions which empower law enforcement authorities to compel information from those in charge of any 'computer resources'. Reciprocally, 'intermediaries' – including ISPs and websites - are within the ambit of the new Rules under the IT Act for co-operating with government agencies on issues or matters of financial liability.
3. Code of Criminal Procedure defines the scope of police powers of investigation which include powers to interrogate and summon information.
4. Individual subscribers enter into contracts with ISPs and web services which do not offer any stringent assurances of privacy with regard to the IP Address details.

Section 43A of the Information Technology Act – Compensation for failure to protect data: -

"Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, not exceeding five crore rupees, to the person so affected".

Explanation-

1. "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may be deem fit.

Indian Cyber Forensics - Indian approach to cyber forensics has not been very encouraging. Despite many claims and promises, Cyber forensics in India has still not evolved suitably as per the need of the dynamic society.

The absence of 'Best Practices and Cyber Forensics' methodology in India has resulted in Improper use of Cyber Forensics for legal, Judicial and law Enforcement purposes. Thus, it is imperative that strong laws as well as implementation and enforcement mechanisms are incorporated in the system as well as the police and judiciary for efficacious dealing of Cyber - Crime issues. Further, the privacy and confidentiality of data of users is of utmost importance and the ISP's should be heavily penalized for disclosing the same to any third party without explicit orders of the Court.