INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions ofthe authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner whatsever for any consequences for any action taken by anyone on the basis of information in theJournal.

Copyright © International Journal for Legal Research & Analysis

 ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur.Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time &Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

 ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN: 2582-6433

INTELLECTUAL PROPERTY THEFT BY EMPLOYEES IN A IT FIRM

AUTHORED BY - RUPSA MUKHERJEE

ABSTRACT

In the evolving landscape of Information Technology (IT) industry, Intellectual Property plays a very important and concerning role which often becomes a cornerstone in the industry. Intellectual property encompasses legal rights to the owner which arises from the creation of various IPs sometimes unknowingly by the firm which provides the firm with huge advancements and advantages. IP is just not an asset but it fuels the economy of the company and helps it securing a place in the market. The protection of intellectual property in IT industry is paramount as the value of intangible assets like software, algorithms, technological solutions are protected which sometimes outweighs the physical assets of the firm. Prevention of such IP theft by the employees has become a rising concern for the IT firms which directly impacts their business as a whole from innovations, producing assets, maintaining clients and daily working of the firm. Safeguarding these intangible assets from theft shall become one of the top priority of such IT firms to maintain their business and their brand name in the market. This paper talks about the primary causes of IT theft by the employees leading to how such theft impact the financial health of the firm. Further the paper talks about how the firms with remote work environment has a contributing factor in increasing such IP thefts and how the firm shall prevent such mishaps and mitigate IP thefts. The paper further discusses how to protect the firm using the legal precedents, laws related to IPs and how a company can apply them in cases of IP thefts. It is crucial for IT companies to implement strong IP protection strategies which contains of strong agreements, employee training, cybersecurity measures and enforcement of IP rights. Lastly, a culture of respect for intellectual property within the organization is very necessary and staying alert against both internal and external threats, is essential. In a globalized digital economy, a strong regime to maintain IP is not just a legal necessity but a strategic method for long-term success.

KEYWORDS

Intellectual Property Theft, IP theft in IT companies, Data theft, IT security and IP protection, Trade secret theft, Software piracy, Employee misconduct, Cybersecurity, Legal consequences

 ISSN: 2582-6433

of IP theft, Protecting innovation in companies, Unauthorized access, Confidential information breach, Intellectual property rights enforcement, Cross-border IP infringement

INTRODUCTION

In the evolving landscape of Information Technology (IT) industry, Intellectual Property plays a very important and concerning role which often becomes a cornerstone in the industry. Intellectual property encompasses legal rights to the owner which arises from the creation of various IPs sometimes unknowingly by the firm which provides the firm with huge advancements and advantages. IP is just not an asset but it fuels the economy of the company and helps it securing a place in the market. The protection of intellectual property in IT industry is paramount as the value of intangible assets like software, algorithms, technological solutions are protected which sometimes outweighs the physical assets of the firm.

All the IT firms deals with Intellectual Property including Patents, Copyrights, Trademarks, Designs and Trade Secrets. The software, algorithms, computing methodologies of the company usually falls under the ambit of Patents which protect their innovations and uniqueness providing exclusive rights over the novel product or process which the owner can use, license, sell or destroy[1]. Talking about Software codes, Databases, Websites and Digital media of a company which is covered under Copyrights of the company. It safeguards the source codes of the software and prevent unauthorized copying. The brand name of the firm is protected under Trademark which protects the Name, Logo and other identifiers that distinguish the company from others and provide the firm with a unique position in the market. [2]For protecting the aesthetic designs of the products manufacture by the firms such as user interface (UI) of the software applications or User Experience (UX) the company can claim design rights for safeguarding their designs and using them as their assets. [3]

As the IT industry is driven by the innovation and intellectual property being an exclusive right providing factor to the firm IP theft is a common mishap which can occur in the industry which makes the industry not only losing rights over their Intellectual Property but also face huge

[1] (*Bluescope Steel Limited (ACN 000 011 058) v Kelly [2007] FCA 517 - Barnet Jade*) <https://jade.io/article/6091>
[2] Mitrofanskiy K, 'Intellectual Property Software: Why Is It Essential' (*Intellisoft*, 28 July 2024) <https://intellisoft.io/what-is-the-technology-that-protects-the-intellectual-property-rights-of-software/>
[3] (*Bluescope Steel Limited (ACN 000 011 058) v Kelly [2007] FCA 517 - Barnet Jade*) <https://jade.io/article/6091>

 ISSN: 2582-6433

economic loss which also brings down the reputation and position in the market.[4] This theft is commonly done by the employees of the industry itself as they are the people who have the maximum information of the company. Employees have close access to the sensitive information of the company and in the position to steal or misuse proprietary knowledge for personal gain by selling it to the competitors.[5] This act can be unintentional or deliberate but regardless of any reason behind the theft it has a serious consequence. Losing rights over the exclusivity of the uniqueness of the industry leads to substantial financial losses, damages to the competitiveness edge of the company and even legal battles. With a rise of remote work, cloud storage, global collaboration the potential of IP has grown exponentially over the years. Downloading, copying and transferring such sensitive information has become easy for the employees which is accessible to them.

Prevention of such IP theft by the employees has become a rising concern for the IT firms which directly impacts their business as a whole from innovations, producing assets, maintaining clients and daily working of the firm. Safeguarding these intangible assets from theft shall become one of the top priority of such IT firms to maintain their business and their brand name in the market. This paper talks about the primary causes of IT theft by the employees leading to how such theft impact the financial health of the firm. Further the paper talks about how the firms with remote work environment has a contributing factor in increasing such IP thefts and how the firm shall prevent such mishaps and mitigate IP thefts. The paper further discusses how to protect the firm using the legal precedents, laws related to IPs and how a company can apply them in cases of IP thefts.

THE HISTORY AND OVERVIEW OF INTELLECTUAL PROPERTY THEFT IN DIGITAL AGE

IP theft is very old crime when the concept of patents and copyrights were emerging in the market in 1700s. It was the first statute to provide that copyright shall be regulated by the government and courts, rather than by private parties." Over the time, IP theft has changed drastically with the evolving technologies. These new digital age brings out significant opportunities for innovation but at the same time increased the risk and fraud frequency of

[4] Terrey R, 'The Impact of Copyright Infringement on Businesses and Individuals' (*Business Coaching, Training & Community for Business*, 17 April 2024) <https://www.the-entourage.com/blog/the-impact-of-copyright-infringement-on-businesses-and-individuals>

[5] 'Top Ip Theft Statistics and Stories in 2023' (*Cyberhaven*) <https://www.cyberhaven.com/guides/top-ip-theft-statistics>

 ISSN: 2582-6433

Intellectual Property. With the reference to cloud computing, digital storage, and rise of remote work environment the theft by employees also evolved making it difficult for the organisations to control and prevent access over their valuable assets. [6]

Cloud Computing and IP theft: Cloud computing enables users to store and access the data over the internet and provides the IT firms with cost efficiency and scalability and is often used for storing sensitive information, data, source code, algorithms and business intelligence[7]. These stored data can be accessible from anywhere in the world which attracts firms for using such technologies creating new vulnerabilities. The employees especially working in remote work environment, are in maximum contact with all the vulnerable information of the company and hence the likelihood of data leakage or misuse has increased. It includes downloading of proprietary software, copying secret information and strategies which being stolen can make the business face huge losses.

Digital Storage and Unauthorized Access: In this digital age, the most significant change is shifting the physical storage into digital storage for handling sensitive information which reduced the use of papers and misplacing them but now with the advent of digital storage the prior was more easily monitored and safe. [8]The sensitive information of a business is stored digitally in databases, servers, and local storage devices which are connected to a wider network, increasing the risk of unauthorized access. Data encryption, access controls and auditing systems have become a critical task in this digital world to protect such IPs against unauthorized access.

Remote Work and Insider Threats: The rise of remote work has fundamentally shifted how businesses operate, accelerated from the COVID-19 pandemic. With flexibility it has also introduced challenges in securing IPs of a company. The office networks are considered to be the secured networks for dealing with sensitive information but in this remote work culture, [9]the employees working from home or any other off- site locations may not use a protected

[6] 'What Is Intellectual Property Theft' (*Thales Cloud Security Products*) <https://cpl.thalesgroup.com/software-monetization/what-is-intellectual-property-theft.
[7] 'Securing Intellectual Property (IP) in the Cloud: CSA' (*Securing Intellectual Property (IP) in the Cloud | CSA*) <https://cloudsecurityalliance.org/blog/2023/08/08/secrets-of-securing-intellectual-property-ip-in-the-cloud>
[8] Bakharev N, Hofesh B and Dizdar A, 'Unauthorized Access: Risks, Examples, and 6 Defensive Measures' (*Bright Security*, 25 March 2025) <https://www.brightsec.com/blog/unauthorized-access-risks-examples-and-6-defensive-measures/>
[9] 'The Risk of Remote Working and Insider Threats: Technical Solutions to Manage Your Workforce ' (*Securonix*) <https://www.securonix.com/blog/technical-solutions-remote-working-and-insider-threats/>

 ISSN: 2582-6433

network or device which makes it easy for cybercriminals to exploit vulnerabilities. Also, all the employees are not well versed with all the safety measures they must follow to keep the information safe while working which is a contributing factor in cybercrimes.

These are some of the ways how sensitive information becomes vulnerable to cyber frauds and causes huge losses to the company where the employee unintentionally contributes towards the IP theft in the firm. Continuing to it, the next part deals with the aspects when the employees intentionally causes IP thefts in their place of working which leads to wide-ranging consequences for the business. Understanding the causes which makes the employees causing IP thefts is a crucial aspect for developing strategies to prevent them.[10] Although every situation is a unique one, several common reasons which contributes in employees committing theft in the IT sector are discussed further.

Financial Gain and Personal Motivation: This is one of the direct cause for IP theft by an employee. Particularly in highly competitive industries like IT, employees get tempted to steal proprietary information which may be source codes, software algorithms, customer database which they further sell or use them for personal gains. Such employees, mostly sell the information to save themselves from direct legal consequence and also to get huge monetary benefits. Some of them use such stolen IP to enhance their own career by using the proprietary technology for self-gains. Proper remuneration and credit provided by the company can somehow reduce such incidents.

Dissatisfaction with Employer: Employees who feels undervalued, have lack of job satisfaction, recognition, who are underpaid or overlooked within their organisation may resort to IP theft as a way to express frustration to their employer. This often happens when an employee feels undervalued in the company, especially in highly creative roles where the work directly leads to new innovations, creating IPs for the firm as a compensation. These types of theft can be prevented by giving proper recognition to the employees for working efficiently for the company and also rewarding them for a success which the company gained through the employee.

Lack of Awareness or Understanding of IP Rights: The employees sometimes unable to

[10] 'What Is Intellectual Property Theft' (*Thales Cloud Security Products*) <https://cpl.thalesgroup.com/software-monetization/what-is-intellectual-property-theft>

 ISSN: 2582-6433

understand, what value the Intellectual Properties contain for the company thus they may believe that taking company data, such as codes, designs, client lists are harmless, for personal use or for further requirements in their career. Such employees might not recognize the consequences of theft, believing that the company's innovations are freely available or that taking some information which would give personal gains is not a crime[11]. For avoiding such instance, a company must conduct sessions where they educate the employees about what is IP and how it adds value to the company. The sessions shall also contain information about, how using IPs of the company for personal use or gains can lead them to suffer criminal proceedings against them leading to huge penalties for stealing IPs of a company. The company shall make their employees understand that even if they are creating any IP for the company, the company is the owner of the rights gained through such creations and not the employees themselves.

Access to Sensitive Information: For many people, opportunity to commit a crime is a driven force for them to actually indulge into it. In many IT Firms, employees, in the technical role have easy access to the valuable proprietary information which are source codes, algorithms, customer data and many more information which are valuable IPs for the company[12]. This occurs mostly when a company do not have sufficient security controls such as inadequate monitoring systems, access restrictions or data encryptions when employees can easily download, copy and also sell such valuable information leaked. A lack of employee monitoring system, weak enforcement of NDAs and poor IT Securities also works as an contributing factor in IP Theft by the employees. The companies shall have an idea about the value, The IPs add to the company and shall restrict the use of such valuable information and also keep a track on all such important and sensitive information.

Cultural and Ethical Lapses and External Pressure: Sometimes, organisations has a history of cutting corners, weak ethical standards, or a work environment where IP theft is considered to be a minor offence, in that case employees having good knowledge about IPs and what values they contain, takes the advantage of the weak culture and use them for personal growth. The company must, strictly convey that IP theft is a crime and any person including employees if

[11] Team SI-E, 'IP Awareness and IP Understanding: Bridging the Gaps' (*Sagacious IP*, 5 April 2023) <https://sagaciousresearch.com/blog/ip-awareness-vs-ip-understanding/>

[12] 'Committing Crime' (*Committing Crime - an overview | ScienceDirect Topics*) <https://www.sciencedirect.com/topics/computer-science/committing-crime>

 ISSN: 2582-6433

caught committing a IP theft, would suffer through legal consequences[13]. In some cases, the employees of a company are coerced, persuaded, pressurized or even incentivized by the competitors to commit IP theft. Sometimes, the competitors pressurize the new employees to disclose confidential information and in return they are offered with hefty amounts or lucrative positions in the company.

IMPACT OF IP THEFT ON IT FIRMS

Intellectual Property theft can cause severe consequences in terms of both, financial losses and reputational damages. In IT Industries, where intangible assets like software, algorithms, and designs contributes as lifeblood of a company's value, IT Theft can hinder innovations, erode stakeholder trust and undermine the company's competitive advantage.

Direct Financial Losses: The immediate financial impact falls in the loss of revenue opportunities as when the sensitive data regarding the IPs of the company, competitors often use, reproduce or sell software codes, IPs and trade secrets, leading to huge losses in the market shares. For many IT companies, the very first product they sell are the software codes and algorithm solutions. IP theft can also result in the loss of future business and strategic opportunities. IT firms rely on their proprietary and intellectual property assets to establish licensing agreements, partnerships, joint ventures with other companies. However, if a firm's IP is stolen, it become less attractive to the partners or clients, who questions the company's ability to safeguard the assets. In 2014**, APPLE** filed a lawsuit against its former employee **Xiaolang Zhang** who was accused of stealing APPLE's trade secrets related to one 'Project Titan' which was an autonomous vehicle technology. After six (6) years when he already left the company the case came to an end where the accused was sentenced to 120 days of prison followed by 3 years of supervised release by the U.S. Magistrate Judge Virginia K. DeMarchi for violation of 18 U.S.C. § 1832. He also paid a sum of $146,984 to Apple. [14]

Legal Costs: The company may face huge legal costs on litigation, settlements and actions in case of a IP Theft and mismanagement in the company. This not only affect the company's financial health but also have long-term implications for its operational and strategic direction.

[13] 'Ethics at Work: An Employer's Guide' (*CIPD*, 21 March 2023) <https://www.cipd.org/en/knowledge/guides/ethics-work-guide/>

[14] 'Former Apple Employee Indicted on Theft of Trade Secrets' (*Northern District of California | Former Apple Employee Indicted On Theft Of Trade Secrets | United States Department of Justice*, 17 July 2018) <https://www.justice.gov/usao-ndca/pr/former-apple-employee-indicted-theft-trade-secrets>

 ISSN: 2582-6433

If an IP theft is committed in an IT Firm, whether by an employee, or external person, it often needs to take proper legal action to protect its assets, damages, and prevent further infringement[15]. These legal processes are both time-consuming and expensive which creates a substantial financial burden. Even if the company wins the company faces financial strain in the ongoing years of the proceedings.

1. Litigation Expenses- One of the primary legal costs involved in an IP theft is the expense associated with litigation. When a firm discovers that its intellectual property has been stolen, it engages itself into lengthy and costly legal proceedings to seek justice and compensation. This involves hiring of attorneys, engaging witnesses, and going through various court proceedings for long.[16]
    - Attorney Fees: IP theft cases often require specialized attorneys who are experts in intellectual property law. The hourly fees for these legal experts are comparatively higher than for general litigation lawyers and the longer the case drags on, the more expensive it becomes in terms of attorney fees.
    - Court Fees and Filing Costs: Filing lawsuits and various legal documents incurs court fees, which can quickly add up, particularly in complex cases that involve multiple filings and jurisdictions.
    - Travel and Administrative Costs: If the legal case involves multiple jurisdictions (such as different states or countries), the company may need to bear the costs of traveling to attend hearings, meet with lawyers, or consult with experts. These costs can put burden for smaller firms.
2. Forensic Investigations and Expert Witness- In cases of IP theft, companies often engage in forensic investigations to gather evidence of the committed theft to trace the origin and determine the scope of the infringement. Digital forensics specialists, cybersecurity professionals, and intellectual property auditors are hired to investigate the documents, who was responsible.[17]
    - Forensic Costs: These investigations often require specialized skills and tools, and the cost of hiring experts in cybersecurity, data forensics, and IP auditing can be significant.

[15] 'Oppression and Mismanagement in a Company' (*cleartax*) <https://cleartax.in/s/opression-mismanagement>
[16] 'The Hidden Costs of an IP Breach: Cyber Theft and the Loss of Intellectual Property' (*Deloitte Insights*) <https://www2.deloitte.com/us/en/insights/deloitte-review/issue-19/loss-of-intellectual-property-ip-breach.html>
[17] Administrator A, 'Tracing the Trail of IP Forensic Analysis' (*Asia IP*) <https://asiaiplaw.com/section/in-depth/tracing-the-trail-of-ip-forensic-analysis>

 ISSN: 2582-6433

- Expert Witnesses: In addition to forensic experts, the firm may need to engage expert witnesses to testify in court about the value of the stolen IP or the harm caused by the theft. These experts help in proving the damages and the nature of the IP theft, but their fees are high and expert witness fees can be too much to pay, which depends on the capacity of the company and also the complexity of the case.

3. Settlement and Licensing Fees - Not all IP theft cases result in lengthy litigations. In many instances, companies try to resolve these disputes through settlement negotiations rather than long litigation proceeding. Settlement helps the companies to avoid the expense of a trial, but still involves huge costs, which are:
    - Settlement Costs: If the company agrees to a settlement in the case of IP theft, it have to make financial dealings in the form of a reduced settlement amount or may have to agree to non-disclosure clauses.
    - Licensing Fees: In some cases, a company may choose to license its stolen IP back to the infringer or a competitor as part of the settlement to avoid further litigation or to generate some revenue from the stolen asset.

"The famous case of **Microsoft and Google** is in the wind since 2010 over royalties related to Xbox game console and smartphones from Motorola Mobility, which was owned by GOOGLE until January 2014, when it sold it to Lenovo but kept many of its patents related to it. The companies did not disclose the financial terms of the deal worked together to strengthen the defence of intellectual property which is according to a Bloomberg report."[18]Although the cases were settled between them both the companies involved extensive legal and investigative costs.

Loss of revenue from stolen IP: The original company whose IPs are stolen, they losses their revenue return streams. The stolen IPs are used by other companies to create their own similar products at a lower cost which undermines the original company's position in the market. In **Google LLC v. Oracle America, Inc**., Oracle claimed that google had infringed their copyright on Java Application Programming Interface (API) code which the US Supreme Court ruled in favour of google under "Fair Use" leading to huge loss of revenue from the IP

[18] Statt N, 'Google and Microsoft End Patent Battle and Drop Lawsuits' (*The Verge*, 30 September 2015) <https://www.theverge.com/2015/9/30/9428345/google-microsoft-patent-fued-end>

 ISSN: 2582-6433

which the company lost. [19]

BRAND REPUTATION

Brand reputation is the most valuable assets in any firm, in the competitive and innovative IT industry. When IP theft occurs, it leads to huge damages to the brand image and reputation. As consumers, clients, partners, and even employees place considerable value on trust, security, and integrity, IP theft poses threat to the foundation of a firm's image[20]. The negative consequences of an IT theft can ripple through the marketplace, which affects the ability of the firm to retain customers, attract new clients, and maintain positive relationships with partners and investors.

Trust is the cornerstone of the relationship between the company and its customers, in the IT sectors, clients often trust companies with their sensitive and personal data, intellectual assets, and confidential information and when a firm's IP is stolen, it depicts to customers that the company's security measures and safeguarding processes may be weak and this breach in trust can result in:

1. Customer Attrition: Customers may feel that their own information is at risk if a company's IP, a crucial part of its product or service offering, is compromised. Clients, therefore, have the ability to walk their business away from that firm and put it in more secure hands, if they so choose. The company's share price can fall as a result.
    - Lower Customer Trust: If a company can't secure their own IP, it seems pretty likely they can't secure your data or other proprietary assets. This trust in being lost may see customers jumping the business ship and taking up with something trustable and a little more secure.
    - Customer Perception of Instability: When news of the IP theft hits, customers might think of the company being in a precarious position. This could create more organisational vulnerability and weakening the long-term contracts or partnerships with the company.

[19] User M, 'Google, Microsoft Resolve Global Patent Fight over Phones, Xbox' (*Marin Independent Journal*, 28 July 2018) <https://www.marinij.com/2015/09/30/google-microsoft-resolve-global-patent-fight-over-phones-xbox/>

[20] 'The Importance of Brand Reputation' (*Templafy*, 6 March 2025) <https://www.templafy.com/brand-reputation/#:~:text=A%20brand%20reputation%20is%20simply,numerical%20terms%20is%20more%20challenging.>

 ISSN: 2582-6433

2. Damage to the Firm's Image as an Innovator

   In the IT industry, innovation is a primary source of success and a method of competition from other competitors. Firms depends on products, services, and technologies to establish them as competitor in their field. IP theft, involves critical technological assets and proprietary software which severely damages the firm's image[21].

   - Perception of Compromised Innovation: IP theft undermines the perception that a firm is capable of maintaining exclusive control over its innovations. If competitors can easily overcome a firm's proprietary technology or intellectual property, it may bring down the company's status as an innovator and could also result in the loss of competitiveness in the market.
   - Stagnation in Product Development: Companies that face IP theft may also become less willing to share their research, data, or ideas due to fears of future theft. This may lead to slow product development, which again brings down the company's ability to innovate and bring new products and services to market.[22]
   - Public Perception of Weakness: If a company's IP is stolen and exploited by competitors, it may no longer be seen as the source of the innovation but as a victim of other firms that have successfully copied its technology. This weakens the reputation and create the perception that the company is no longer capable of protecting its properties and creations.[23]

3. Impact on Relationships with Partners and Stakeholders

   - Technology companies frequently depend on strategic partnerships, joint ventures, and alliances with other types of companies, including technology suppliers and investors. Such relationships are based trust and a common objective in the development and safeguarding of intellectual property. The occurrence of IP theft then breeds distrust and insecurity, which can subsequently disrail existing as well as future partnerships.[24]

[21] 'How It Can Damage Your Image, Reputation, and Business' (*FasterCapital*) <https://fastercapital.com/topics/how-it-can-damage-your-image,-reputation,-and-business.html>

[22] India R, 'Case Study: Technology Risks – Intellectual Property Theft and Product Obsolescence' (*Risk Management Association of India*, 30 January 2025) <https://rmaindia.org/case-study-technology-risks-intellectual-property-theft-and-product-obsolescence/>

[23] Ezell S and Cory N, 'The Way Forward for Intellectual Property Internationally' (*RSS*, 3 June 2022) <https://itif.org/publications/2019/04/25/way-forward-intellectual-property-internationally/>

[24] Mutambik I, 'The Role of Strategic Partnerships and Digital Transformation in Enhancing Supply Chain Agility and Performance' (*MDPI*, 29 October 2024) <https://www.mdpi.com/2079-8954/12/11/456>

 ISSN: 2582-6433

- Loss of Trust Among Partners: After experiencing IP theft, a company is likely to face reevaluation of its relationships by partners, suppliers, and investors. These stakeholders would perhaps think that the theft was an indicator in o the company's inability that would eventually lead to financial loss, legal issues, or loss of identity.
- Negative impact of the mismanagement: The key factor in a relationship between a company and its client is the trust on the company's management. If the theft is caused due to mismanagement, lack of vigilance, or ineffective security practices, of the firm, the reputation of the company can severely harm. This can lead to further damaging the company's position in the market.
- Losing future trust and deals: Potential business deals, licensing agreements, or joint ventures may get cancelled as the prior mismanagement is continuously remembered. Reputation is a driving factor which maintains the balance between the customer trust and the company. It not only tarnishes the reputation but also tends to dismantle future deals and can suffocate long-term contracts with a firm whose intellectual property is at risk of theft.

4. Public Relations and Media Perusal

   When IP theft occurs, it involves high-profile technologies and has a large-scale impact. This canattract media coverage which can affect the firm in a negative tone, with news which highlights the firm's failure to protect its intellectual property. The increased media influence and negative publicity leads to:

   - Impact of the Press: Press coverage of IP theft caused in the company frames the company as irresponsible and negligent towards the most confidential information of the company even if the firm is a victim and an external agency caused such activity. The competitors make sure the victim company losses the intellectual property which can lead to widespread negative reputation of the company.[25]
   - Social Media Counterblast: In this digital age, the social media flashes the news to leakage of the data from the company which creates dissatisfaction or disbelief over the company's inability to protect its intellectual property. This can harm the reputation of the fimr in a long term.

[25] Meet the Expert Chris Brook Editor, 'IP Theft: Definition and Examples' (*Fortra's Digital Guardian*, 22 August 2024) <https://www.digitalguardian.com/blog/ip-theft-definition-and-examples>

 ISSN: 2582-6433

- Loss of Customer Confidence: Negative press and social media reviews highlights the firm's failure to protect their IP, confidential information and consumer private data which increases the concerns over privacy and security. This can damage the company's products or services which are linked to sensitive data, such as financial software or cloud-based services.

5. Long-Term Recovery Challenges

Once a brand's reputation has been damaged the recovery can be very long and expensive. The longer it takes to restore the consumer's trust, the more time the company would take to revive the old reputation and overcome challenges related to declining sales, lost customers, and difficulty in attracting new clients. [26]Brand recovery after IP theft requires significant efforts in the following areas:

- Rebuilding Trust: Regaining customer trust may involve expensive campaigns, customer outreach and shall guarantee stronger future protections. These efforts, can bring back the trust but immediate restoration of consumer confidence is very tough.
- Strengthening Security and Transparency: Companies will often need to demonstrate their commitment to preventing future theft by implementing stronger cybersecurity measures and being more transparent about their IP protection strategies. This can involve public statements or the development of new security protocols, which may be expensive and time-consuming.
- Time and Cost of Rebuilding Brand Value: Beyond direct financial costs, the company may need to invest heavily in rebranding and marketing to change the public's perception. In cases of severe IP theft, advertisements, media appearances, and corporate sponsorships might be required to restore a positive brand image, all of which come at a cost.

In the case of **Tesla v Zoox (2020)** Zoox, an autonomous driving company, was accused of hiring former employees of Tesla, who took the proprietary information with them, led to a loss of trust in Zoox's ability to create original innovations, damaging their reputation in the tech community[27].

[26] Aguiar M and others, 'From Crisis to Comeback: The Long Road to Rebuilding Corporate Trust' (*BCG Global*, 7 April 2025) <https://www.bcg.com/publications/2024/rebuilding-corporate-trust>

[27] Intellepedia and others, 'Tesla Files Lawsuit against Ex-Employees and Zoox, Apple-Google's COVID-19 Tracking Plan Faces Data Security Threats and More' (*Intellepedia*, 27 April 2020) https://www.bananaip.com/intellepedia/tesla-files-lawsuit-against-ex-employees-and-zoox-apple-googles-covid-19-tracking-plan-faces-data-security-threats-indian-government-addresses-covid-19-apps-privacy-concerns-and-mo/>

 ISSN: 2582-6433

MARKET POSITION AND INNOVATION

IP theft can undermine a firm's ability to maintain its competitive edge in the marketplace. It includes proprietary technologies, algorithms, source code, trade secrets, software and product designs. When a firm invests in its research and development, it relies on its IP to differentiate itself in the market. IP theft can severely impact a firm's ability to maintain this competitive edge, which leads to several strategic consequences. [28]

1. Loss of technological differentiation: A company's proprietary technology or innovations are often the key selling points that distinguishes its products from its competitors. IP theft allows rivals to access and replicate these technological innovations, causing the original company's product less unique and consequently attractive to consumers.
2. Erosion of Market Share: With the stolen IPs the rivals can easily make a copy of the design, source code or trade secrets and the original company would be left behind with nothing. This also leads to erosion of market share of the company if the stolen IP allows the competitor to offer a superior product at a lower cost or with the stolen features. In the **Apple v. Samsung** patent infringement case, Apple sued Samsung for copying the design of its product, iPhone. In such condition if a company steals the design, it would have been able to produce similar products at a lower price, which results in lowering the shares of the original company. [29]
3. Market confusion and consumer trust: Stolen IP, particularly in the form of product designs or functionalities, can create market confusion which would lead to confuse the customers as well. When a competitor replicates a product's feature or design it would also try to produce a more innovative thing to produce it in the market which can dilute brand identity and erode brand loyalty, especially if the copied product is cheaper or more easily available.

Impact on employees and workplace culture: IP thefts results in far beyond of just financial losses or legal consequences, it also significantly affects employee morale and the overall workplace culture within the IT company. When IP theft occurs within an organization, which is committed by someone in a position of trust, it can create a toxic environment where

[28] Chekanov K, 'Best Ways to Protect Intellectual Property in Outourcing' (*Artkai* , 31 March 2025) <https://artkai.io/blog/intellectual-property-theft-in-outsourcing>

[29] Kastrenakes J, 'Apple and Samsung Settle Seven-Year-Long Patent Fight over Copying the iPhone' (*The Verge*, 27 June 2018) <https://www.theverge.com/2018/6/27/17510908/apple-samsung-settle-patent-battle-over-copying-iphone>

 ISSN: 2582-6433

employees feel unsafe, suspicious, and demotivated to work.[30] The immediate reaction from other employees might be distrust and anxiety and they question whether their own ideas or work could be stolen next. The situation is damaging when the perpetrator is a colleague who was seen as part of the team. Employees who work hard to protect their intellectual creations starts to feel that the organization does not adequately value or protect their contributions, leading to a sense of undervaluation. Over time, this results in betrayal towards the organisation as a whole who fails to address the IP theft committed inside the firm. The firm must take measures which are transparent and supportive. When the trust on the ability of the company and the management of the company declines, no longer the company is seen as a reliable guardian to protect their intellectual property. When the trust in leadership reduces, it becomes difficult in collaborating and also entertains negative work culture, which is very important for the company where creativity and innovation can gain success and maintain a position in the market. It also helps the company to maintain a high turnover rate. The collaborative spirit is very necessary for creative innovation in IT firms and this IP theft decline the quality of teamwork and communication which makes it more difficult for the organization to innovate and solve problems.

PREVENTIVE MEASURES

Intellectual property is always been a cornerstone in innovation and competitive advantage of IT firms. To ensure that valuable technology, designs, and other intellectual assets are protected, IT companies must have a strategy to prevent IP theft. This management strategy involves legal protections, technological measures, employee awareness, and internal policies. [31]

1. **Establish Clear IP Ownership Policies**

   One of the ways to prevent IP theft is to set policies that are be said to all employees. This includes software, designs, inventions, and other works which are developed as part of their job. Including **non-compete clauses** and **non-disclosure agreements (NDAs)** within these contracts can protect such creations to prevent the theft and legal implications. When employees are aware that their creations belong to the company and they have legal responsibilities to protect this intellectual property they try not to

[30] Interns I, 'Impact of Intellectual Property Theft on the Economy' (*Intepat IP*, 19 November 2022) <https://www.intepat.com/blog/impact-of-intellectual-property-ip-theft-economy/>

[31] Tran B, 'The Importance of IP Education for Employees' (*PatentPC*, 29 March 2025) <https://patentpc.com/blog/the-importance-of-ip-education-for-employees>

 ISSN: 2582-6433

misuse or steal it.

- Non-Disclosure Agreements (NDAs) and confidentiality clauses are important tools which protects intellectual property in of the company, particularly in the IT industry where trade secrets, software, and technologies are at high risk. NDAs are legally bonded contracts which prohibit employees from disclosing or misusing confidential information and data of the firm. NDAs in the IT industry often protects source code, software, client lists, business strategies, and other sensitive data. If employees try to breach these agreements, the employer can take legal action against them and can claim damages.
- Employment Contracts: Employment contracts in India are essential to establish clear guidelines regarding the ownership of intellectual property in the firms. These contracts include clauses that mentions the employer's rights over all the IPs created during the employment of the employee. They may also refer to the clauses related to confidentiality and the non-compete to prevent employees from theft and working for competitors or using company IP after leaving the firm.

2. **Implementing Security Measures**

IT firms should implement advanced data encryptions methods and firewalls to protect digital assets. Sensitive intellectual property like source code, product designs, and sensitive information should only be accessed by the employees. This controlled access ensures that employees can only access the information necessary for specific works and to avoid unauthorized access. A multi-factor authentication and regular monitoring of network activity can also help in preventing unauthorized access on important data. IT firms should regularly conduct audit to ensure safety against the cyber threats. The data loss prevention (DLP) helps in monitoring and protecting data exploitation when employees attempt to extract the ata and transfer them through external devices or cloud platforms. [32]

3. **Employee Education and Awareness**

Employees play a vital role in protecting intellectual property of the company. Regular training and awareness programs should be conducted to educate them and make them understand the importance of IP, the company's policies regarding IP ownership, and the consequences of theft. These programs include topics such as the proper handling

[32] 'What Is DLP (Data Loss Prevention)?: Guide to DLP Security' (*Palo Alto Networks*) <https://www.paloaltonetworks.com/cyberpedia/what-is-data-loss-prevention-dlp>

 ISSN: 2582-6433

of confidential information and the legal obligations for stealing IP.[33] Educating the staffs about their rights and obligations in the company towards the IPs of the company. They should understand the legal obligations and consequences of breaching those protections. Responsibility and ethical behaviour can reduce the chances of accidental and intentional theft.

4. **Make a strong Hiring and Exit Processes**

   During the hiring process the IT firms should perform proper background identifications to ensure that the employees have a clear history regarding intellectual property rights. It very important for the company to hire senior employees who would have the access to sensitive information. Screening is must to identify past IP theft or disputes which can help the management in resolving the risk to company's assets.

   Firms should ensure that exit interviews are conducted with their employees when they are leaving the company. In these interviews, the employees shall be reminded of their confidentiality to which they are obligated as per the contracts to perverse the intellectual property of the company. Employers should ensure that the company assets, such as laptops, source codes, typical software are duly returned by the employees. Data shall also be erased from the devices of the employee before leaving the company to ensure protection of the data.

5. **Conducting Regular Audits and Security Assessments**

   Periodic audits of the company's systems, employee activities, and intellectual property can prevent them from thefts. This include proper documentation and limited access to the information. Regular assessments can also detect signs of misconduct, unusual file transfers and unauthorized attempts to access confidential data

6. **Implement a Clear and Secure IP Management System**

   IT companies should adopt a structured IP management system to ensure all intellectual property is documented and tracked. This can be achieved by using IP management software that can track the creation, ownership, and usage of IP assets of the company. A proper management system can protect the IP easily and any unauthorized use can be identified. Having a record of all IP assets makes it easier to enforce legal protections and obligation to resolve disputes regarding IP theft.

[33] 'Educating Employees on Intellectual Property: Why It Matters' (*ELLIPSE*) <https://www.ellipseip.com/educating-employees-on-intellectual-property-why-it-matters/>

 ISSN: 2582-6433

LEGAL AND REGULATORY FRAMEWORK IN INDIA

This paper further talks about the Legal and regulatory Framework in India which protects the Intellectual properties of IT firms[34]. India has a valuable legal and regulatory framework to protect intellectual property which ensures that the companies safeguard their innovations, inventions, designs, and trade secrets. These laws and conventions balances the protection of IP and also addresses employee rights in IT firms India's IP laws are largely based on the global standards and international conventions like World Trade Organization (WTO) and Trade-Related Aspects of Intellectual Property Rights (TRIPS). This legal framework governs the protection of patents, copyrights, trademarks, and trade secrets.

- **Patents**: Under the Indian Patents Act, 1970 an employee makes an invention in the course of the employment. The patent rights are owned by the employer if the invention is related to the employee's work and if the employee was hired specially to create such inventions. Employees, generally require to assign their rights to the employer as part of their employment agreement.
- **Copyrights**: Under the Copyright Act, 1957, the copyright for work created by an employee in the course of employment which belongs to the employee-employment contract. This applies to software, creative content, and other works produced during work hours or as part of assigned duties.
- **Trade Secrets**: Trade secrets are primarily protected under common law principles related to breach of confidence and contract law. Employees who have access to confidential information or trade secrets are legally bound to not to disclose such information without consent from the employer. In India, trade secret protection is not fully covered under a specific law but is governed by the Indian Contract Act, 1872 and the Indian Penal Code (IPC) when there is a breach of confidentiality.

INTERNATIONAL CONVENTIONS AND FRAMEWORKS

India is a signatory to several international agreements and conventions that regulates the IP rights and ensures that the country's legal framework are aligned with international standards.

- TRIPS Agreement (World Trade Organization): This agreement establishes minimum standards for the protection of intellectual property rights globally, including patents, copyrights, trademarks, and trade secrets. India is committed to ensuring that its IP laws

[34] 5, 'India - Protecting Intellectual Property' (*International Trade Administration | Trade.gov*) <https://www.trade.gov/country-commercial-guides/india-protecting-intellectual-property>

 ISSN: 2582-6433

conform to TRIPS standards, ensuring legal protection for IP at both national and international levels.

- WIPO (World Intellectual Property Organization): India is a member of WIPO, which helps provide a framework for resolving international disputes related to IP theft and infringement. WIPO's conventions, like the Patent Cooperation Treaty (PCT), also offer avenues for international patent protection, which may be relevant in cases of IP theft across borders.[35]
- Berne Convention: As a member of the Berne Convention, India ensures the protection of literary and artistic works, including software, which is a significant concern for IT firms.
- This can be understandable by referring to legal cases which the companies can refer as precedents which would help them to understand complexities of IP theft which would also work as preventive measures which an IT firm can avoid to prevent such IP theft in their organisation.

Info Edge (India) Pvt. Ltd. And Anr. vs Shailesh Gupta And Anr. 98 (2002) DLT 499

In this case the plaintiff adopted the name 'NAUKRI.COM' in 1997 and since then he was carrying a business under the aforesaid domain name. in 1999 the defendant registered two domain names which are 'JOBSOURCEINDIA.COM' and 'NAUKRI.COM' which was identical to the domain of the plaintiff. When the plaintiff filed a suit against the defendant for passing off and also claimed ad-interim relief.

The court's legal reasoning pivots on the concept of passing off- it happens when someone deliberately passes of their goods or services as those belonging to another party. This action of misrepresentation damages the goodwill of the party whose goods or services are misrepresented causing huge monetary losses to the person or business. In this case the defendant used the domain name of the plaintiff with mala-fide intension (act of bad faith) to capitalize on the plaintiff's goodwill. The court also mentioned it as a IP theft of the domain name of the company for the defendant's own good. The court also referred to several pivotal cases to establish the legal framework for domain name protection.

[35] Admin, 'International Treaties Applicable to Indian IPR Laws: A Comprehensive Overview' (*BETTERING RESULTS*, 23 December 2024) <https://betteringresults.in/international-treaties-applicable-to-indian-ipr-laws-a-comprehensive-overview/>

 ISSN: 2582-6433

The judgement stands as a pivotal reference in the realm of trademark law and protection, particularly concerning digital assets of the company like domain name. the court also bolstered the legal framework safeguarding the brand against online impersonation and deceptive practices. The court also mentioned the necessity for the businesses to vigilantly protect their online Intellectual properties which are the asssets to the businesses.

Mondelez India Pvt Ltd. V Neeraj Food Products 142 (2007) DLT 724[36]

This case involves a dispute between Mondelez India Pvt. Ltd. (Cadbury)and Neeraj Food Products where Cadbury who sells a well-known product, button chocolates covered in colourful candy shells under the famous Trademark – 'GEMS' and 'GEMS BOND'. The defendant Neeraj Food Products launched a similar product naming 'GEMS' or 'GEMS BOND' or 'JAMMY BOND' using the similar packaging style which can confuse the customers on a large scale. Cadbury filed a case against the defendant for causing trademark and copyright infringement as their design and the product is similar to that of the plaintiff.

The Delhi High Court ruled in favour of Cadbury' Gems as it is widely known and famous product to the general public and any other name or similar product can confuse the customers on a large scale which can also harm the goodwill of the product of Cadbury. The Court also used the principle of Res Ipsa Loquitur (the thing speaks for itself) owing to the similarities between both products, releasing the plaintiff from the burden of proving the same.

Yahoo!, Inc. v. Akash Arora & Anr. 1999 IIAD Delhi 229, 78 (1999) DLT 285[37]

In this case, the plaintiff (Yahoo! Inc.) filed a suit seeking permanent injunction against the defendants who used their service as 'yahooIndia' on the domain name of yahooIndia.com which was very identical to the trademark of the plaintiff. The plaintiff had exclusive rights on the trademark and the domain name of YahooIndia and the defendant committed passing off by manipulating consumers at large and hence damaging the goodwill of the plaintiff.

The court remarked that it was an act of passing off which is an intellectual property theft which was committed by the defendant knowingly to harm the reputation and affect the goodwill of the plaintiff. Therefore, the court granted injunction and prevent commercial use

[36] Manupatra, 'Manupatra' (*Articles*) <https://articles.manupatra.com/article-details/Case-Analysis-of-Mondelez-India-Foods-Pvt-Ltd-V-Neeraj-Food-Products-Cadburys-Gems-Vs-James-Bond>

[37] Sampathkumar S, 'Yahoo Inc v. Akash Arora' (*IP Matters*, 25 August 2021) <https://www.theipmatters.com/post/yahoo-inc-v-akash-arora>

 ISSN: 2582-6433

of it and passing it off.

CONCLUSION

Intellectual Property theft creates threat to the It companies and All the IT firms deals with Intellectual Property including Patents, Copyrights, Trademarks, Designs and Trade Secrets. The software, algorithms, computing methodologies of the company usually falls under the ambit of Patents which protect their innovations and uniqueness providing exclusive rights over the novel product or process which the owner can use, license, sell or destroy such creations. This theft is commonly done by the employees of the industry itself as they are the people who have the maximum information of the company. Employees have close access to the sensitive information of the company and in the position to steal or misuse proprietary knowledge for personal gain by selling it to the competitors[38]. Brand reputation is the most valuable assets in any firm, in the competitive and innovative IT industry. When IP theft occurs, it leads to huge damages to the brand image and reputation. As consumers, clients, partners, and even employees place considerable value on trust, security, and integrity, IP theft poses threat to the foundation of a firm's image. The negative consequences of an IT theft can ripple through the marketplace, which affects the ability of the firm to retain customers, attract new clients, and maintain positive relationships with partners and investors. [39]Intellectual property is always been a cornerstone in innovation and competitive advantage of IT firms. To ensure that valuable technology, designs, and other intellectual assets are protected, IT companies must have a strategy to prevent IP theft. This management strategy involves legal protections, technological measures, employee awareness, and internal policies. It is crucial for IT companies to implement strong IP protection strategies which contains of strong agreements, employee training, cybersecurity measures and enforcement of IP rights. Lastly, a culture of respect for intellectual property within the organization is very necessary and staying alert against both internal and external threats, is essential. In a globalized digital economy, a strong regime to maintain IP is not just a legal necessity but a strategic method for long-term success.

[38] '12 Different Types of Employee Theft (with Examples)' (*AllVoices*) <https://www.allvoices.co/blog/12-types-of-employee-theft-with-examples>
[39] Nguyen ST, 'Protecting Personal Information: A Guide for Business' (*Federal Trade Commission*, 2 April 2024) <https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business>