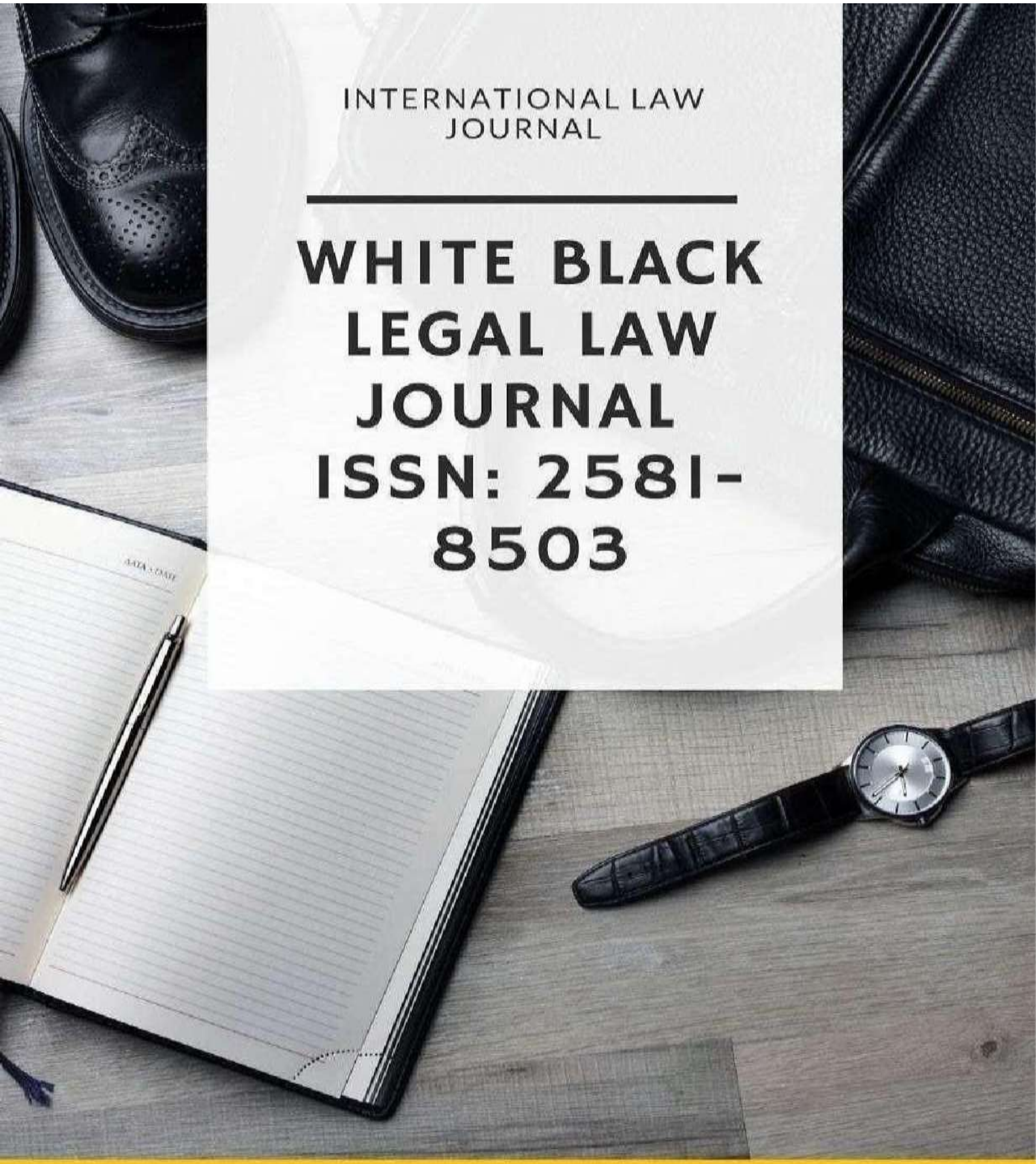

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi, Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur,
M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

UNMASKING BRAND COUNTERFEITING IN THE SHADOWS OF SOCIAL MEDIA MARKETING

AUTHORED BY - MEERA M & MEDHA K N

The social media and society have taught us to consume fashion by setting unreasonable standards and in order to feel accepted, people tend to purchase high end luxury brands or designer products.[1] Conventionally these brands are only affordable to the upper class while the middle, working and the lower classes go for popularly priced products which are a counterfeit, this has resulted in the rise of brand counterfeiters. These counterfeiters were easily tracked down by the brand proprietors in virtual commerce and wired marketing platforms such as Amazon, Flipkart, Ajio, Meesho, etc. But these pretenders have found a brand-new intact method to peddle these items through a platform called social media marketing (SMM). With the help of various fashionistas, influencer and bloggers these products are being promoted and with the edge of cut-rate prices they make a lot of profit with an overall brand equity of the original product. Additionally, they also face the intricacies of managing online reputation, mitigating unfavourable reviews and keeping abreast of the rapid shifts in the digital arena. But the brand proprietors are grappling with issues through cyber space such as tackling counterfeit items, addressing brand impersonation, fortifying against data breaches, and upholding consistent brand presentation across a wide array of plugged in platforms. To make matters worse, many of these counterfeiters employ Virtual Private Networks (VPNs) to hide their tracks, making it challenging for law enforcement and brands to track them down. In this article, we will delve into the world of brand counterfeiting through social media marketing and explore how the social media platforms and the virtual private networks (VPNs) can be regulated under the existing law of India.

[1] Sun, Y, Wang, R, Cao, D & Lee, R 2021, 'Who are social media influencers for luxury fashion consumption of the Chinese Gen Z? Categorisation and empirical examination', Journal of Fashion Marketing and Management, vol. (In-Press), pp. (In-Press). https://dx.doi.org/10.1108/JFMM-07-2020-0132

THE RISE OF SOCIAL MEDIA COUNTERFEITING:

Social media platforms have given counterfeiters a global stage to showcase their counterfeits. These platforms, such as Facebook, Instagram, and Twitter, allow counterfeiters to create sophisticated and convincing online stores. They use high quality images, persuasive marketing and often hijack authentic branded content to deceive unsuspecting consumers.

Counterfeiters use the lure of low prices and eye-catching advertising to trick customers into purchasing counterfeit products. These products range from counterfeit luxury fashion items to counterfeit electronics and medicines. The consequences of these frauds can be devastating for both consumers and legitimate businesses, including lost sales, damaged brand reputation, and potential health risks from substandard products.

THE VPN-SHEILD:

One of the biggest challenges in the fight against social media-based counterfeiting is the use of VPNs by counterfeiters. A VPN is a tool that allows users to mask their IP address and encrypt their internet traffic, making it nearly impossible to trace your online activity to your specific location. Counterfeiters use her VPN to create a cloak of anonymity that protects them from detection and prosecution.

The use of VPNs by counterfeiters poses a multifaceted problem for brands and law enforcement, making it difficult to determine the geographic origins of counterfeiting activity and complicating litigation and international cooperation. As a result, counterfeiters often operate with relative impunity and pose a constant threat to both brands and consumers.

HOW THESE COUNTERFEITERS PEDDLING THROUGH E-COMMERCE WERE TRACKED DOWN?

Brand counterfeiters on platforms like Amazon, Flipkart and Meesho are tracked down and brought to justice using various legal and investigative methods:

1. **Brand Investigative Work**: Many brands are We actively monitor online marketplaces for counterfeit products containing our trademarks. They will hire investigators or work with

authorities to identify sellers offering counterfeit products.

2. **Marketplace Policies and Reporting**: Online marketplaces like Amazon and Flipkart have strict policies against counterfeit products.
3. **Secret Purchases**: Brands or investigators may make secret purchases from sellers of suspected counterfeit products to obtain evidence of counterfeit products.
4. **Criminal Prosecution**: In cases involving large-scale counterfeiting or significant economic loss, law enforcement may bring criminal charges against the counterfeiter. International cooperation and coordination among law enforcement agencies was critical to the detection and prosecution of these criminals.
5. **Use of Technology**: Brands and researchers use technology tools and services to monitor online marketplaces, track product listings, and identify sellers involved in counterfeiting.
6. **Anti-counterfeit programs**: Many brands have established anti-counterfeit programs that include partnerships with investigators, legal experts, and technology companies to proactively combat counterfeit products on online platforms.

Notable cases that have made headlines in the past include brands such as Apple, Nike, and Louis Vuitton taking legal action against sellers of counterfeit products on various online market places.These lawsuits typically result in settlements or court decisions that set legal precedents to combat counterfeit online products.

TRACKING DOWN BRAND COUNTERFEITERS BEFORE THE ADVENT OF VIRTUAL COMMERCE:

Involves different investigative methods and challenges. Here are some ways counterfeiters were pursued in the pre-digital era:

1. **Physical Market Surveillance**: Law enforcement agencies and brand representatives conducted physical surveillance of local markets, street vendors, and retail stores to identify and seize counterfeit products. This often required on-the-ground investigations.
2. **Informants and Whistleblowers**: Informants and whistleblowers from within the counterfeiting networks or the public were valuable sources of information. They provided

tips about counterfeit operations and the individuals involved.

3. **Undercover Operations**: Investigators and brand representatives sometimes went undercover to infiltrate counterfeit networks. They posed as buyers or employees to gather evidence and information about the counterfeiting operations.
4. **Supply Chain Tracing**: Brands traced the supply chain of counterfeit goods by examining invoices, shipping records, and distribution networks. This helped identify the source and flow of counterfeit products.
5. **Marking and Packaging Analysis**: Counterfeit products often had distinctive markings, packaging, or labelling that differed from genuine items. Analysing these details helped in identifying counterfeit products and their source.
6. **Raids and Seizures**: Law enforcement agencies and brand representatives conducted raids on warehouses, manufacturing facilities, and distribution centers suspected of producing or storing counterfeit goods. Seized counterfeit products served as evidence.
7. **Consumer Complaints**: Complaints from consumers who unknowingly purchased counterfeit products played a role in identifying counterfeiters. These complaints often led to investigations and legal actions.
8. **Collaboration with Customs**: Brands collaborated with customs and border protection agencies to intercept counterfeit goods at international borders. This helped prevent counterfeit products from entering the market.
9. **Legal Action**: Brands pursued legal action against counterfeiters through civil lawsuits for trademark infringement, copyright violation, and related charges. Successful cases resulted in injunctions and damages.
1. 10.**Public Awareness**: Brands often launched public awareness campaigns to educate consumers about the risks of counterfeit products and how to identify genuine items. This reduced demand for counterfeit goods.
10. **Industry Associations**: Industry associations and trade groups played a role in sharing information and coordinating efforts to combat counterfeiting. They often had dedicated committees or task forces for this purpose.
11. **Cooperation with Law Enforcement**: Brands and investigators worked closely with law enforcement agencies to share information, evidence, and expertise, leading to arrests and prosecutions.

While the methods used to track down brand counterfeiters in the pre-digital era were different from today's digital methods, the core principles of investigation, collaboration, and legal action remained essential in the fight against counterfeiting. Advances in technology and changes in commerce have shifted the landscape, but counterfeiting remains a persistent challenge that requires ongoing vigilance and innovation in enforcement efforts.

LEGAL AND POLICY ANALYSIS ON REGULATION OF VPNs:

Below is a comparative legal analysis of VPN regulations in some countries, including India: [2]

1. **United States**: VPNs are legal in the United States. VPNs typically take a simple approach and are often used for privacy and security reasons. Although there are no federal laws that specifically regulate VPNs, data protection laws and regulations affect your data protection and privacy.
2. **China**: VPNs are highly regulated in China.
   The Chinese government strictly regulates VPN services.
   Unauthorized VPN services are prohibited and only government-approved VPNs are allowed.
   - Great Firewall: The "Great Firewall of China" monitors and restricts Internet access, and VPNs are often used to circumvent these restrictions.
3. **Russia**: VPNs are legal in Russia and there are laws requiring VPN providers to register with the government.
   Providers must comply with censorship requests and store user data for a certain period of time.
4. **European Union**: VPN is legal in the EU.
   VPN services are governed by the GDPR (General Data Protection Regulation) and your privacy and data protection are our top priorities.
   However, there are no specific EU-wide regulations regarding the use of VPNs.
5. **UK**: VPN is legal in the UK.
   Although the UK has data protection and privacy laws, there are no specific regulations for VPNs.
6. **Iran**: VPNs are generally illegal in Iran.

[2] https://www.forbes.com/advisor/business/are-vpns-legal/

Iran has strict regulations against using VPNs that are not approved by the government. The purpose is to control and monitor Internet access.

7. **Turkey**: VPNs are legal in Turkey, but Turkey has regularly blocked access to certain VPN services, especially during political events.
   The country has regulations that require ISPs to block access to certain content.
8. **Australia**: VPNs are legal in Australia and there are data retention laws that require ISPs to store user data.

However, there are no specific laws covering the use of VPNs.
VPN is legal in **India**. Although there is no specific law regulating VPNs, the government has the power to block or restrict VPN services under the IT Act.Temporary bans on VPNs occur in cases of social unrest or security concerns.

Common Trends:
Several countries, including Russia and Australia, have implemented or considered data retention laws impacting VPN services. Countries with strict internet censorship, like China and Iran, often regulate VPNs to control access to information. Many regions, such as the EU with GDPR, emphasize strong data protection laws that indirectly impact VPN services.

Divergent Approaches:
China exercises significant control over VPNs for censorship purposes, while other countries take a more permissive stance. The EU places a strong emphasis on user privacy, contrasting with countries that implement data retention laws.

REGULATING VPNs:

The classification of VPNs as *intermediaries* under the IT Act, 2000, offers a regulatory framework that can balance the legitimate needs of users for privacy and security with the imperative to address potential misuse for illegal activities.

Regulating Virtual Private Networks (VPNs) under the Information Technology (IT) Act, 2000, falls

under the category of intermediary regulation.[3]

VPNs provide a service that facilitates the transmission of electronic records over the internet. VPNs, on behalf of users, receive, store, and transmit electronic records by encrypting data and facilitating secure connections. This aligns with the IT Act's definition of intermediaries, emphasizing their role in handling electronic records on behalf of users.

VPNs act as intermediaries between users and the internet.[4] Users subscribe to VPN services to access the internet securely, and VPN providers process electronic records on behalf of users, establishing a clear user-agent relationship.

The IT Act imposes certain obligations on intermediaries, such as the requirement to cooperate with law enforcement agencies, take down unlawful content, and maintain user data. If VPNs are considered intermediaries, they may be subject to similar legal responsibilities.[5]

Also in several jurisdictions, VPN providers are considered intermediaries and are subject to regulations governing their activities. Recognizing VPNs as intermediaries aligns with international practices and legal standards.

To combat cybercrime and illegal activities facilitated by VPNs, regulations can mandate data retention policies for VPN providers. This would ensure that they retain user data for a specified period, facilitating cooperation with law enforcement agencies during investigations. While intermediaries are regulated, there is an inherent balance between security and privacy. Regulation can be designed to ensure that VPNs adhere to specific security standards without compromising user privacy beyond what is necessary for legitimate law enforcement purposes. The IT Act aims to regulate and facilitate electronic transactions while addressing issues related to electronic records. Recognizing VPNs as intermediaries aligns with the act's objective of overseeing entities that play a role in the electronic ecosystem.

[3] Section.79 of the Information Technology Act,2000

[4] https://mybalancetoday.com/navigating-the-digital-shadows-unveiling-the-realm-of-faceless-cc-socks-vpns-and-proxies/

[5] The Information Technology (intermediary guidelines and digital media Ethics Code) Rules,2021

Regulating VPNs under the IT Act allows for a holistic approach to cybersecurity, considering the role they play in both facilitating secure communication and potential misuse for illegal activities. Recognizing VPNs as intermediaries enables policymakers to distinguish between legitimate and illegitimate uses. Regulatory measures can be crafted to address illegal activities while ensuring that VPNs continue to serve their essential purposes, such as safeguarding online privacy and enhancing cybersecurity.

In conclusion, the classification of VPNs as intermediaries under the IT Act, 2000, offers a regulatory framework that can balance the legitimate needs of users for privacy and security with the imperative to address potential misuse for illegal activities

REGULATING SOCIAL MEDIA:

Regulating social media platforms under the Information Technology (IT) Act, 2000, for brand counterfeiting involves recognizing the responsibilities these platforms bear in the digital ecosystem.

The IT Act defines intermediaries as entities that provide services with respect to electronic records.[6] Social media platforms act as intermediaries by facilitating the transmission, storage, and sharing of electronic records, including content related to brand counterfeiting.

Social media platforms have significant control over the content shared on their platforms. They can moderate and control the material posted by users. As per the IT Act, intermediaries have the responsibility to exercise due diligence in ensuring that the content hosted on their platforms complies with the law.[7]

Social media marketing often involves user-generated content, including posts and advertisements. When these user-generated contents promote or involve brand counterfeiting, social media platforms become facilitators of potentially illegal activities, falling under the purview of the IT Act.

Social media platforms engage in the storage and transmission of electronic records, including data

[6] Section.2(w) of Information technology Act,2000
[7] Section.79 of the Information technology Act, 2000

related to brand counterfeiting. This aligns with the definition of intermediaries in the IT Act, making them subject to certain obligations and liabilities.

The IT Act provides a legal framework for online platforms to ensure responsible conduct. It outlines the obligations of intermediaries, including the requirement to promptly remove or disable access to unlawful content. Brand counterfeiting, being an illegal activity, falls within the scope of content that platforms should regulate. The marketing and sale of counterfeit products on social media can pose risks to consumers. Regulating social media platforms under the IT Act allows for addressing consumer protection concerns, aligning with the Act's objectives to safeguard users' interests.

Many jurisdictions globally have implemented regulations or standards that hold social media platforms accountable for the content hosted on their platforms. Recognizing the international trend, aligning with the IT Act would help maintain consistency with global practices.

Social media platforms, as powerful entities with significant influence, have a corporate responsibility to ensure that their platforms are not used for illegal activities such as brand counterfeiting. Regulation under the IT Act reinforces the notion of corporate accountability. Social media platforms can be instrumental in mitigating brand impersonation, a common tactic employed by counterfeiters. Regulating these platforms under the IT Act provides a legal framework for addressing issues related to brand impersonation and protecting the intellectual property of genuine brands.

Social media platforms have advanced technological capabilities that allow them to monitor and control content. Regulating them under the IT Act acknowledges these capabilities and empowers platforms to take proactive measures against brand counterfeiting.

While these arguments support the regulation of social media platforms under the IT Act for brand counterfeiting, it's essential to balance regulatory measures with considerations for free speech, privacy, and the role of social media in fostering legitimate commerce. Regulatory frameworks should be carefully crafted to address illegal activities while respecting fundamental rights and promoting responsible business practices.

CONCLUSION:

Brand counterfeiting through social media marketing has been a challenge for brands and consumers alike. This is due to the use of Virtual Private Networks (VPNs) to hide their tracks, making it difficult for law enforcement and brands to track them down. Brand proprietors are grappling with issues such as tackling counterfeit items, addressing brand impersonation, fortifying against data breaches, and upholding consistent brand presentation across a wide array of plugged in platforms. The use of VPNs by counterfeiters presents a multifaceted problem for brands and law enforcement, making it challenging to identify the geographical origin of the counterfeit operation. Brand proprietors are grappling with issues such as tackling counterfeit items, addressing brand impersonation, fortifying against data breaches, and upholding consistent brand presentation across a wide array of wired platforms.