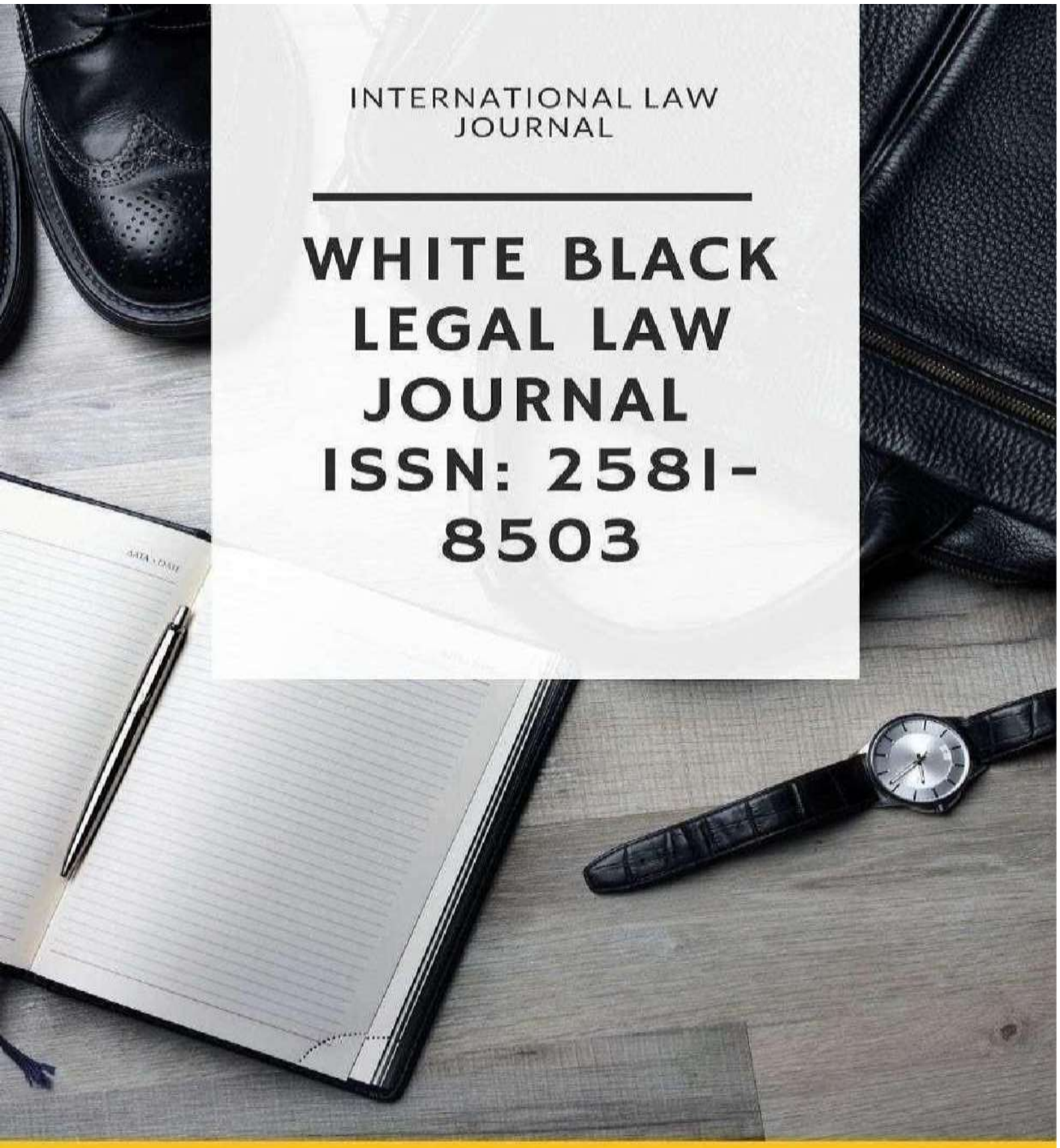

INTERNATIONAL LAW JOURNAL

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

EXAMINING THE LEGAL BOUNDARIES OF ONLINE ANONYMITY

AUTHORED BY - DR. NEWAL CHAUDHARY[1]

Abstract:

Online anonymity has become a contentious issue as the internet pervades more aspects of everyday life. Anonymity provides both cover for criminal activity and protection for free speech, complicating finding an appropriate legal balance. This paper examines the legal boundaries and regulations surrounding internet anonymity through comparative analysis of approaches in Nepal, the United States, the European Union, and other relevant countries. The paper begins by discussing the role of anonymity in facilitating harmful vs. socially beneficial activities. Cyberbullying, dangerous speech, copyright piracy are contrasted with examples like activists evading authoritarian states. Next, the paper explores laws governing anonymous speech, including Constitutional protection of anonymity in the U.S. and E.U. standards on prohibiting mandatory identification. Differing legal perspectives on privacy as a right versus a privilege are analyzed. The paper compares regulations and court cases involving voluntary anonymity in social media, anonymity requirements in financial transactions, and compelled identification of anonymous speakers. Examples from Nepali law are drawn from the Electronic Transaction Act and Right to Information Act. Global debates around encryption are discussed in light of its role enabling online anonymity. Additionally, the paper examines standards required for legally piercing anonymity through court subpoenas, including relevant precedents from Nepal, India, and the U.S. Finally, proposed reforms are considered, such as limiting overuse of subpoenas or requiring exhaustion of other remedies first. The paper concludes that while online anonymity facilitates misdeeds, moderate regulations grounded in rule of law may strike the most appropriate balance between online freedoms and protections.

Keywords: Harassment, Whistleblowing, Right to be forgotten, Cyberbullying, Encryption, Free speech.

[1] Advocate, Supreme Court of Nepal ; Assistant Professor , Nepal Law campus, Tribhuvan University, Exhibition Road, Kathmandu, Nepal. Email: nc2067@gmail.com

I. Introduction:

The internet has opened up unprecedented opportunities for anonymous communication and online activity. Individuals are able to speak, publish content, and browse the web without disclosing their real-world identity. This anonymity has enabled beneficial forms of free expression and privacy as well as provided cover for harmful illegal behavior. As internet use continues growing across commerce, politics, and social contexts, lively debates have emerged surrounding the appropriate legal boundaries for online anonymity. The cloak of anonymity provided by the internet has allowed people to explore interests, express opinions, and engage in discussions without fear of judgement or retaliation. Minorities and vulnerable groups have used anonymity to share their experiences and find community when they could face discrimination if their identities were known. Anonymity enables citizens under oppressive regimes to criticize leaders and mobilize resistance without facing punishment. Dissident anonymous blogging and social media organizing played a major role in the Arab Spring protests that toppled dictators. Anonymity also facilitates whistleblowing and speaking truth to power. Government and corporate corruption can often only be exposed through anonymous leaks. Major scandals like Watergate first came to light through unnamed sources that would have faced severe retaliation if identified. Anonymous tip lines allow people to report crimes without jeopardizing their safety. Anonymity provides oversight and accountability for abuses of authority that otherwise would remain hidden. However, anonymity can also provide cover for harmful and illegal behavior without accountability. Cyberbullying by anonymous trolls has driven vulnerable individuals to suicide. Compromised privacy for victims of revenge porn, leaked medical records, or financial fraud can lead to extreme trauma. Dangerous speech and disinformation spread rapidly when masked by anonymity. Copyrights and trademarks are infringed on a mass scale by anonymous pirates. Child pornography and other abusive content is harder to regulate when distributors cannot be identified. Law enforcement cites the difficulties anonymity poses for investigating online drug and arms trafficking, solicitation of minors, and terrorist radicalization. Victims of harassment, stalking, defamation, and data theft can be left without legal recourse if their anonymous tormentors cannot be unveiled. Some experts argue anonymity enables a permissive environment for extremism and societal degradation. Others counter that forfeiting online privacy is too high a price for an uncertain increase in security. Where exactly to legally delineate between protections for legitimate uses of anonymity and interventions to prevent abuse remains hotly contested worldwide. Complicating factors like jurisdictional disagreements, technological workarounds, and clashing cultural values around privacy make crafting consistent global standards elusive. As the internet reshapes human relations, governments, legal scholars, tech

companies, and citizens wrestle with balancing order and openness, freedom and accountability. How society adapts legal boundaries around online anonymity could significantly shape digital freedoms for generations to come.

II. Benefits and risks of online anonymity:

Anonymity, and more broadly, the right to use a pseudonym not tied to one's legal name, has been contested for centuries[2]. Online anonymity provides cover for a wide range of socially beneficial activities that promote free expression, privacy, and security against oppression. Under the cloak of anonymity, vulnerable groups are able to explore interests, express opinions, and engage in discussions without fear of judgement, discrimination, or retaliation. This provides protections for minorities, women, LGBTQ individuals, and other marginalized communities to share their authentic experiences and find support when they could face backlash if their identities were known. Dissidents and activists living under authoritarian regimes rely heavily on anonymity to criticize their governments and organize resistance without facing punishment like imprisonment, torture, or execution. The protests during the Arab Spring that led to the toppling of dictators in countries like Tunisia and Egypt were fueled by activists using anonymous blogging and social media organizing to get around state censorship and surveillance. Anonymity provides citizens a powerful tool to challenge oppressive institutions when speaking openly would be met with retaliation. Anonymity also facilitates oversight, accountability, and speaking truth to power by empowering whistleblowing. Government and corporate corruption, abuses of human rights, threats to public health and safety, and other misconduct can often only be exposed through anonymous leaks, confidential informants, and undisclosed data submissions. Major scandals like Watergate first came to light through unnamed sources speaking to reporters, who would have faced severe backlash if identified. Anonymous tip lines allow insiders and observers to report crimes and unethical activities without jeopardizing their own livelihoods and safety. By safeguarding whistleblowers, anonymity gives the powerless some ability to keep the powerful in check, exposing wrongdoing that otherwise would remain hidden. The ability to anonymously share information in the public interest acts as a crucial societal safeguard, increasing accountability and transparency.

However, anonymity can also cloak harmful and outright illegal behavior in a veil of unaccountability. Cyberbullying is bullying that takes place over digital devices like cell phones,

[2] Belfer Center for Science and International Affairs. (2023, March 8). Why online anonymity matters. Retrieved from https://www.belfercenter.org/publication/why-online-anonymity-matters

computers, and tablets. [3]Cyberbullying by anonymous online mobs has driven vulnerable individuals, especially children and teenagers, to depression, anxiety, and even suicide. The spread of dangerous disinformation, conspiracy theories, and character assassination is amplified when propagators cannot be easily identified and held responsible. Anonymous comments can contribute to the rise of extreme political polarization and erosion of civic discourse. Compromised privacy stemming from data leaks, medical record disclosure, revenge porn, financial fraud, and identity theft can lead to severe trauma when victims have no recourse against anonymous perpetrators. Stalking, directed harassment, threats of violence, and recruitment efforts become more dangerous for targets when their tormentors cannot be traced. Law enforcement cites anonymity as a major obstacle to investigating online drug trafficking, arms dealing, solicitation of minors, and terrorist radicalization. Additionally, copyrights, trademarks, and intellectual property are infringed on a massive scale by anonymous pirates. The piracy advocacy site Scihub, hosted on undisclosed servers and domains to evade legal jurisdiction, provides unauthorized free access to over 80 million copyrighted academic articles. Anonymous file transfer sites and torrent trackers enable millions of users to freely, and illegally, distribute films, music, books, and software. This intellectual property theft causes substantial economic harm, depriving creators of royalties and undermining industries. Anonymous activities also complicate content moderation on social platforms, sometimes forcing capitulation to aggressive anonymous mobs. When anonymous groups threatened violence against Facebook employees for banning far-right accounts, citing where they lived, the company had to walk back enforcement to protect workers. Complete online anonymity makes it difficult to balance open platforms against preventing real societal damage from illegal and dangerous content. Anonymity provides both a shield protecting vulnerable groups and oversight of the powerful, as well as a sword allowing misconduct with little accountability. Balancing its benefits and risks remains complex, situational, and debatable. However, anonymity seems likely to remain a permanent feature of the internet landscape, for better or worse. The challenge lies in maximizing its advantages for free speech and privacy while developing safeguards to limit abusive behaviors shielded behind its veil.

[3] U.S. Department of Health & Human Services. (n.d.). What is cyberbullying? Retrieved from https://www.stopbullying.gov/cyberbullying/what-is-it

III. Laws and court cases governing anonymous speech:

The legal right to anonymous speech has roots in the United States Constitution and has been affirmed through numerous court cases. However, this right is not absolute and boundaries have been established through jurisprudence. Courts have balanced protections for anonymity against other interests such as protecting victims and limiting libel. This section will analyze relevant US constitutional principles, Supreme Court decisions, and lower court cases that have shaped the standards for legal protections around anonymous speech. The First Amendment of the US Constitution establishes protections for freedom of speech and expression against government interference. While anonymity is not explicitly mentioned, Supreme Court decisions like McIntyre v. Ohio Elections Commission (1995) have established constitutional cover for anonymous political speech like pamphleting. However, these protections are limited in cases of libel, obscenity, or threats. Courts have ruled compelled identification can be constitutional when required to enforce other laws.

A seminal Supreme Court case dealing with anonymity is McIntyre v. Ohio Elections Commission (1995), which overturned an Ohio state prohibition on distributing anonymous political pamphlets. [4]Justice Stevens wrote this violated the First Amendment by infringing on core political expression. This established constitutional protection for writers to remain anonymous. However, in Holder v. Humanitarian Law Project (2010), the Court upheld a law prohibiting providing material support to terrorist groups, even for peaceful activities like advocacy[5]. This showed anonymity protections have limits when public safety requires identifying speakers. In cases like Doe v. Cahill (2005), courts have delineated standards for when anonymity can be overridden in civil suits. The court ruled that plaintiffs must provide sufficient evidence to meet standards for libel and other laws before compelling the revelation of an anonymous defendant's identity. However, standards differ among jurisdictions. In In re Anonymous Online Speakers (2011), the Ninth Circuit ruled that anonymous online speakers deserved higher standards of protection than offline counterparts. Anonymous speech issues continue to arise around whistleblowing, reviews, and privacy. Many democracies have protections for anonymity, but approaches differ. The European Court of Human Rights ruled in cases like McVicar v. United Kingdom (2002) that free expression rights protected anonymous defamation of public figures[6].

---

[4] McIntyre v. Ohio Elections Commission. (1995). Retrieved from https://www.fec.gov/legal-resources/court-cases/mcintyre-v-ohio/

[5] Holder v. Humanitarian Law Project, 561 U.S. 1 (2010).

[6] Council of Europe, Guide on Article 10 of the Convention – Freedom of Expression (2022), https://rm.coe.int/guide-art-10-eng/16809ff23f.

However, the EU's ePrivacy Directive requires opt-in consent for storing identifying cookies and IP addresses. Anonymity standards remain contested globally between free speech advocates and regulators. Anonymity retains some legal shelter in the US and other democracies but is balanced case-by-case against other rights. As the internet expands what anonymous speech is possible, courts continue to adapt standards in this complex arena.

Nepalese's Law on Anonymous Speech:

- The 2015 Constitution of Nepal guarantees the right to freedom of opinion and expression under Article 19. However, this right can be restricted by existing laws.
- The Electronic Transaction Act (ETA) of 2008 authorizes penalties for persons who use electronic media to publish illegal content. However, it does not directly address anonymity7.
- The Right to Information Act of 2007 established the right to access public information but also protects privacy rights that could enable anonymity.
- The National Cybersecurity Policy of 2016 aimed to enhance cybersecurity and prevent cybercrimes but did not specifically mention anonymity regulation.
- Overall, Nepal's laws do not comprehensively regulate anonymous speech, but some existing provisions could potentially apply. However, protections may be afforded under general constitutional free speech principles.

Nepal Court Cases:

- Nepal's Supreme Court ruled that provisions of the ETA criminalizing online content were unconstitutional violations of free speech. This potentially strengthens protections for anonymous expression.
- However, the Supreme Court has also directed authorities to enact laws criminalizing objectionable social media posts, which could impose restrictions.
- In 2021, the Nepal police arrested three people for alleged anonymous defamatory posts on social media, indicating limited tolerance for abuses of anonymity.8
- But concrete court precedents directly addressing anonymous speech protections remain lacking in Nepal's legal landscape. Enforcement so far has been inconsistent.

---

[7] Electronic Transactions Act, 2063 (2008). http://www.tepc.gov.np/uploads/files/12the-electronic-transaction-act55.pdf.

[8] Cyber Bureau of Nepal Police. (2023, August 12). Nepal Police requests people to refrain from misusing social media. Retrieved from https://nepalnews.com/s/nation/nepal-police-requests-people-to-refrain-from-misusing-social-media

Nepal's jurisprudence on anonymous speech is still evolving. While the Constitution enshrines free expression principles, their application to regulating emerging online anonymity issues remains untested. More court cases and clear laws may be needed to firmly establish boundaries.

IV. Voluntary anonymity on social media platforms:

Social media platforms represent a major arena where anonymity norms are negotiated. Each platform approaches balancing user anonymity with accountability and safety differently based on its community policies. However, regulations and public pressure are increasingly shaping companies' stances on anonymity. This section will overview controversial issues around anonymity on major platforms and how policies handle pseudonymous and anonymous profiles.

Facebook

Facebook requires users to provide their real identities but allows some pseudonymous profiles, causing inconsistencies in enforcement. The company came under scrutiny when anonymous groups used it to spread hate speech, bully, and organize extremism. In response, Facebook has aimed to increase profiling of pseudonymous accounts to enforce real-name policies. However, digital rights advocates have warned this could endanger vulnerable users and curtail free expression. Facebook remains under public pressure from both sides to address harms from anonymity while maintaining privacy.

Twitter

Twitter allows pseudonymous accounts and does not require identity verification, which has led to rampant trolling, misinformation, and harassment. But the platform has resisted calls for blanket real-name requirements due to concerns over enabling repression of dissenting voices, particularly in authoritarian countries. Twitter has focused on reducing abuse through behavior-based interventions like disabling accounts that violate policies against violence, extremism, and Election integrity. But dangerous uses of anonymity persist on its decentralized platform.

Reddit

Reddit grants users a high degree of anonymity, especially on forums like r/darknet discussing illegal activities. This has led to controversies around hosting extremist content. Reddit relies heavily on volunteer moderators to enforce content policies and has enhanced intervention in cases of violence and illegal activity. Overall, Reddit leans towards maximizing anonymity but struggles with defining boundaries to balance it with social responsibility.

Regulations like the EU's Digital Services Act are increasing pressure on platforms to curb abuses of anonymity and illegal content or face large fines. End-to-end encrypted messaging apps like WhatsApp and Signal pose challenges to content moderation by preventing access to data. Synthetic media and AI-generated deepfakes enabled by anonymity represent emerging threats to truth and trust online. Social platforms continue wrestling with the tradeoffs between privacy and accountability when shaping their policies around online anonymity. Handling anonymous and pseudonymous profiles on social media remains an evolving tightrope walk between upholding transparency, free expression, privacy, and security. How platforms choose to navigate these complex waters will likely remain controversial on all sides.

V. Regulations on financial transactions and Anonymity:

Governments worldwide have enacted laws and regulations aimed at limiting anonymity in banking and finance to combat money laundering, tax evasion, terrorist financing, and other illegal activities. However, privacy advocates argue these measures infringe on rights to anonymity and financial privacy. Ongoing debates continue around balancing regulations against risks of overreach. This section will provide an overview of regulations related to financial anonymity and arguments on both sides.

Regulations like Know Your Customer (KYC) and Anti-Money Laundering (AML) laws require banks and financial institutions to collect identifying information on customers like legal names, addresses, dates of birth, and copies of government ID. This is done to detect suspicious transactions and share data on illegal activities with regulators and law enforcement. However, civil liberties groups argue mandatory identification could exclude vulnerable groups from essential financial services.

In the United States, the Bank Secrecy Act empowers the Treasury Department to collect financial data through FinCEN to combat crimes. Banks must file Suspicious Activity Reports on high risk transactions over $10,000.[9] Similar regulations exist globally, but critics argue this Strips Individuals of Privacy rights and anonymity. Financial regulators counter that risks of terrorism and crime outweigh privacy impacts.

The pseudonymous nature of cryptocurrencies like Bitcoin poses challenges to financial regulators. Some countries like China have banned cryptocurrency transactions. Others require

[9] Financial Crimes Enforcement Network. (n.d.). Bank Secrecy Act. Retrieved from https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act

exchanges to implement KYC and transaction monitoring. But privacy-focused cryptocurrencies like Monero allow users to obscure activity, alarming regulators. Calls for outright cryptocurrency bans compete with arguments for nuanced regulations to curb illicit usages without stifling innovation.

Countries are also collaborating more to share financial information and curb tax evasion through agreements like the United States' FATCA law. However, even legal tax avoidance strategies are increasingly under scrutiny. Critics argue opaque offshore banking laws enable abuse by wealthy individuals and money launderers. But directly regulating offshore systems also jeopardizes legitimate uses as well as financial privacy.

Regulations on financial anonymity attempt to balance law enforcement interests with privacy rights. However, lack of global coordination and evolving technologies like cryptocurrency continue to provide avenues for illicit activities. Regulators face difficult tradeoffs between enforcing laws and avoiding intrusive overreach.

VI. Compelled identification of anonymous speakers:

While anonymity is constitutionally protected in certain contexts, its protections are not absolute. Courts have established standards allowing for the compelled identification of previously anonymous speakers when necessary to enforce laws and balance rights. However, digital rights advocates argue these standards are applied overzealously, chilling online speech. This section will examine the legal tests and procedures involved in compelling disclosure of anonymous internet users' identities.

A common method used is issuing a subpoena to online platforms ordering them to provide identifying information about a user to reveal their identity. Standards vary, but generally plaintiffs must convince a judge that identification is needed to pursue legal action and there are sufficient grounds to override anonymity. Critics argue judges grant these subpoenas too readily. Many cases involve libel suits aimed at unmasking anonymous critics. In Dendrite v. Doe (2001), the court established a balancing test requiring plaintiffs to provide: (1) evidence proving unlawful conduct, (2) that the speech caused harm, and (3) the need to override anonymity. Proponents argue this strikes an appropriate balance between rights, but others contend it chills lawful speech[10].

[10] Dendrite Data Corp. v. Doe, 724 A.2d 374 (N.J. Super. Ct. App. Div. 2001).

Some laws, like anti-SLAPP statutes, provide stronger protections for anonymity by allowing early dismissal of suits targeting protected activities like whistleblowing. However, only some jurisdictions have adopted these protections. Some argue federal anti-SLAPP laws are needed to protect anonymity for whistleblowers nationwide.

Approaches differ internationally. In the US, subpoenas are widely used to identify anonymous speakers. However, European courts have imposed higher barriers to compel identification, especially in libel cases. Global technology companies face conflicting pressures across jurisdictions when responding to unmasking orders.

VII. Global encryption debates:

The advent of widespread strong encryption technologies poses significant challenges for regulating online anonymity. Encrypted messaging apps like WhatsApp and Signal allow users to communicate without messages being easily accessible, even with a warrant. This frustrates law enforcement and national security agencies who argue impediments to accessing encrypted data endanger public safety. However, technologists and civil liberties groups counter that encryption provides essential protection for rights including privacy and anonymity. Ongoing debates continue around the world on balancing encryption and anonymity with security.

Some governments have called for encryption backdoors to allow legally authorized access to encrypted data. Australia passed laws allowing compelled technical assistance to intercept communications. The UK proposed weakened encryption standards that were eventually scrapped after backlash. In the US, proposals like the EARN IT Act Would threaten encryption if companies do not aid law enforcement investigations. However, critics argue backdoors weaken overall security and violate rights.

Some repressive regimes like China and Iran have banned encrypted messaging apps, requiring state-approved versions that facilitate surveillance. Russia passed laws requiring decryption assistance citing anti-extremism. But this gives authoritarian government’s excessive power to suppress dissent and invade privacy behind the guise of public safety. Outright encryption bans provide cover for rights violations.

Russia, China, and others have passed “data localization” laws requiring citizens’ data be stored domestically where governments can readily access it for surveillance. This undermines

anonymous communications by exposing data to state authorities. However, these laws also conflict with the global nature of the internet.

Technologies like VPNs and blockchain also allow anonymous users to obscure their locations, frustrating law enforcement and regulators. When anonymous actors span jurisdictions, it becomes unclear whose laws apply, enabling legal gray zones. Emerging decentralized networks like Web3 pose new challenges to regulating anonymity. Encryption and other technologies raise complex tradeoffs between rights, security, and governance. How democracies choose to navigate these issues will likely shape the future landscape of online privacy and anonymity globally.

VIII. Legal standards for piercing anonymity:

While anonymity is protected in many contexts, courts have established standards allowing for compelled identification when balanced against other rights and interests. This section examines the legal tests, burdens of proof, and procedures involved in overriding anonymity protections. It also analyzes standards in different jurisdictions and proposals for reform.

A common method to legally unveil anonymous actors is through a subpoena or court order compelling a platform to identify a user. Plaintiffs typically must demonstrate the claim has legal merit, that anonymity is impeding the suit, and that identification is the only way to advance the case. Defendants can try to quash subpoenas to maintain anonymity. Standards vary among courts. Many attempts to unveil anonymity involve libel suits. In the US, tests like the Dendrite standard require balancing rights by showing: (1) evidence of unlawful conduct, (2) the speech caused harm, and (3) necessity of identification. Critics argue this chills lawful speech. The Cahill test establishes similar factors but a lower evidence bar. Each state differs somewhat in specific standards. Higher barriers exist for identifying anonymous political speakers, given First Amendment protections. In Doe v. Cahill, the court ruled public figure plaintiffs must meet high standards for defamation before compelling identification of critics. Anonymity provides shelter for whistleblowers and dissenters, meriting heightened protections. The US relies heavily on subpoenas to unveil anonymous actors. But European courts have imposed higher barriers, especially regarding libel claims and political speech. The EU “right to be forgotten” also enables anonymity-shielding delisting’s. China and Russia compel far broader identification, subordinating anonymity to state power. Some argue for stronger federal laws limiting subpoena powers and establishing clearly defined standards to protect lawful anonymous speech. Others contend current balancing approaches are appropriate if carefully applied. But anonymity

protections remain debated across jurisdictions. Legal efforts to pierce anonymity require nuanced balancing of rights and interests case-by-case. However, standards vary globally based on differing values around privacy and authority. The bounds of protected anonymity continue to be negotiated through evolving regulations and court precedents.

IX. Conclusion

Online anonymity represents a complex frontier fraught with tradeoffs between beneficial and harmful usages. Anonymity provides protections for free speech, privacy, and vulnerable groups but also shelters foul play ranging from harassment to serious crime. However, anonymity seems inevitable on the internet given technical decentralization and global connectivity. Laws and regulations delineating the boundaries of protected anonymity verses compelled identification remain contested worldwide. Each country differs in navigating tensions between civil liberties, security, and accountability online according to its values and context. Additionally, technological developments continually reshape the landscape of regulating anonymity on the internet. Finding balanced approaches requires nuance. Blunt bans on anonymity would likely undermine democratic principles and stifle innovation. But leaving unchecked anonymity would pose dangers to society. Well-crafted regulations grounded in rights and rule of law may strike a moderate path forward. However, room for reasonable disagreement exists on where to draw the lines. This paper aimed to provide an overview of key debates and analyze relevant laws and court cases that help define the current legal boundaries of online anonymity. Many open questions remain regarding how to maximize anonymity's advantages while minimizing harms. As the internet continues rapidly evolving, societies worldwide will likely grapple with negotiating anonymity protections for generations to come in the search for equilibrium between openness and responsibility. Additional future research could further explore public attitudes on anonymity, examine technical methods for accountability, or propose governance frameworks to address Transborder jurisdictional gaps. But fundamentals like human rights, contextual values, and democratic principles should remain at the center of guiding policy as we navigate this complex digital terrain.