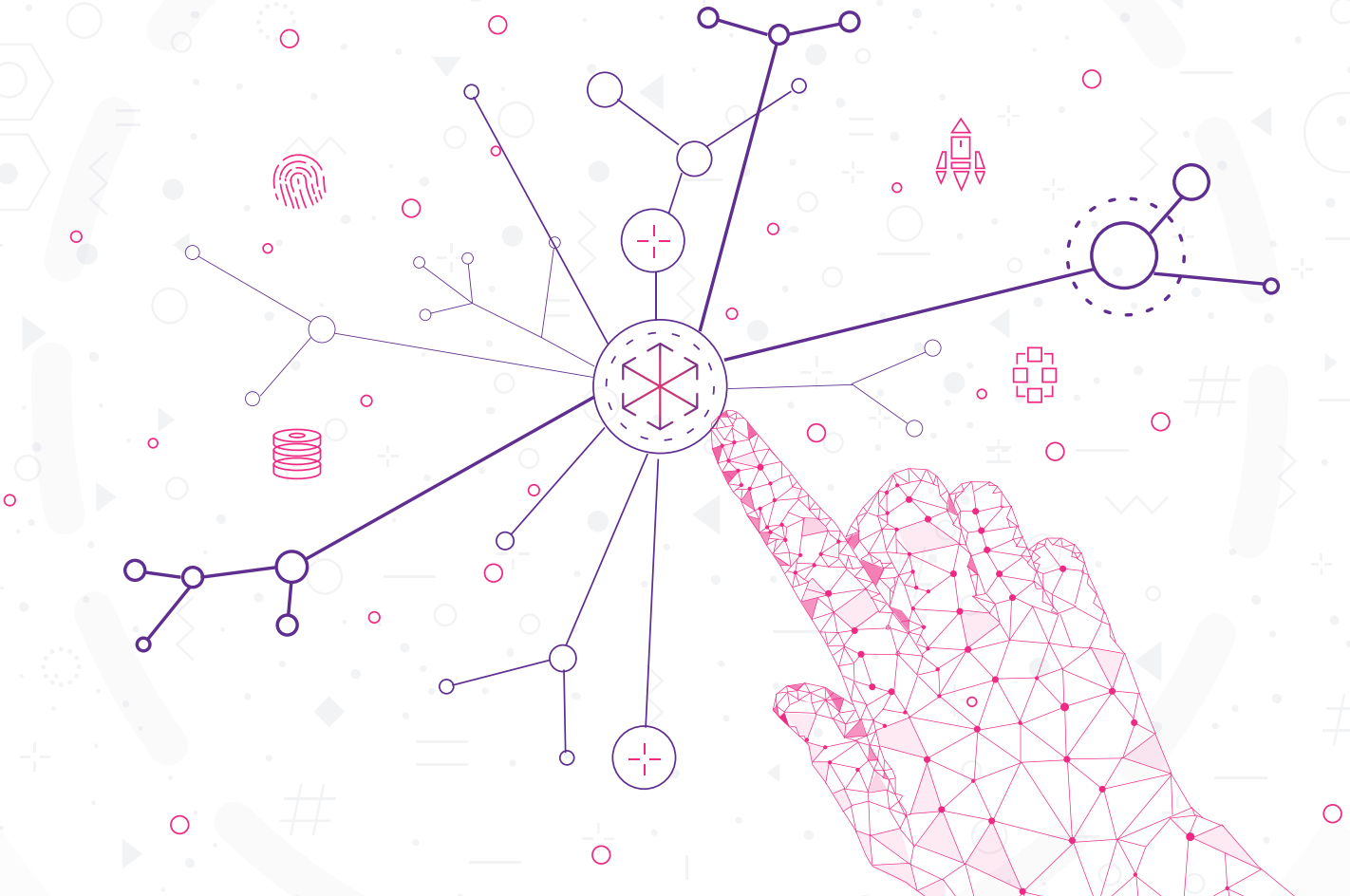
IKIGAI LAW

USER VERIFICATION ON THE INTERNET:

BALANCING ANONYMITY, SECURITY AND INNOVATION



About Ikigai

Ikigai Law is a technology and innovation focused law and policy firm. We have a rich history of working in new and emerging sectors defined by regulatory uncertainty. We work with several of the world's largest technology companies as well as startups, industry associations and the government. Our practice areas include platform governance, data protection, cloud, digital competition, fin-tech, artificial intelligence, among others. Our unique combination of law, public policy and government affairs practice allows us to provide an informed and 360-degree support to our clients. Our practice areas and members of our team have been highly ranked over the years by the India Business Law Journal, and global directories such as The Legal 500 and Chambers and Partners.

Authors

Pallavi Sondhi
Senior Associate
pallavi@ikigailaw.com

Aarya Pachisia
Associate
aarya@ikigailaw.com

Namratha Murugeshan
Associate
namaratha@ikigailaw.com

Aman Taneja
Partner
aman@ikigailaw.com

Index

Executive summary 2

Chapter I: Introduction 4

Chapter II: Exploring user verification and anonymity 9

- Understanding identification, verification and authentication 9
- Unpacking anonymity 11

Chapter III: Evaluating the need for user verification measures on social media 15

- User identity verification in the financial sector 15
- User identity verification in the telecom sector 17
- User verification on social media platforms 17
- To what degree should there be user verification on social media 21

Chapter IV: Exploring user verification in other countries 24

- South Korea 24
- Brazil 25
- United Kingdom (UK) 25
- European Union (EU) 27

Chapter V: Conclusion and recommendations 28

- Principles for online user verification mandates 29

References 31

Executive Summary

Policy proposals for user verification on the internet are gaining momentum across the globe. There is a need to better identify anonymous perpetrators and fake profiles on the internet. Governments are hence considering mandatory user verification on social media platforms, such as – requiring users to disclose their real name or providing official identity documents. However, these proposals have received criticism, for diluting online anonymity, thereby adversely affecting fundamental freedoms such as free speech and privacy of users and being a disproportionate measure to curb online harms. This white paper explores if, and to what degree, should user verification requirements be imposed on social media platforms.

Mandatory user verification is already imposed in sectors such as financial and telecommunication services. However, these services are not used in the same way as social media, which serves as a platform for free expression, political dissent and free press. These freedoms are fundamental to a thriving democracy. Thus, the trade off in introducing strict verification on social media platforms is much higher, because of the adverse impact on speech, anonymity and privacy of users. Mandatory user verification on social media may not pass the constitutional standards of proportionality.

There is also limited empirical data to show that user verification mandates have reduced online harms. In fact, global precedent, such as in South Korea, has shown otherwise. There are also less intrusive alternatives available, which preserve some degree of anonymity of users, while still allowing identification of bad actors, if needed.

For user verification in India, policy makers also need to consider India's demography, societal challenges, digital economy and infrastructure. User verification is cost intensive, which could adversely affect the growth of India's burgeoning tech start-ups and in turn, India's goal of a trillion dollar economy. There are also costs and risks associated with safely storing user data. Further, a majority of India's marginalized population does not have valid identity documents. Identity verification will further restrict their access to the internet. Policy proposals in India should carefully balance these considerations.

Key Principles for User Verification Mandates on Social Media Platforms

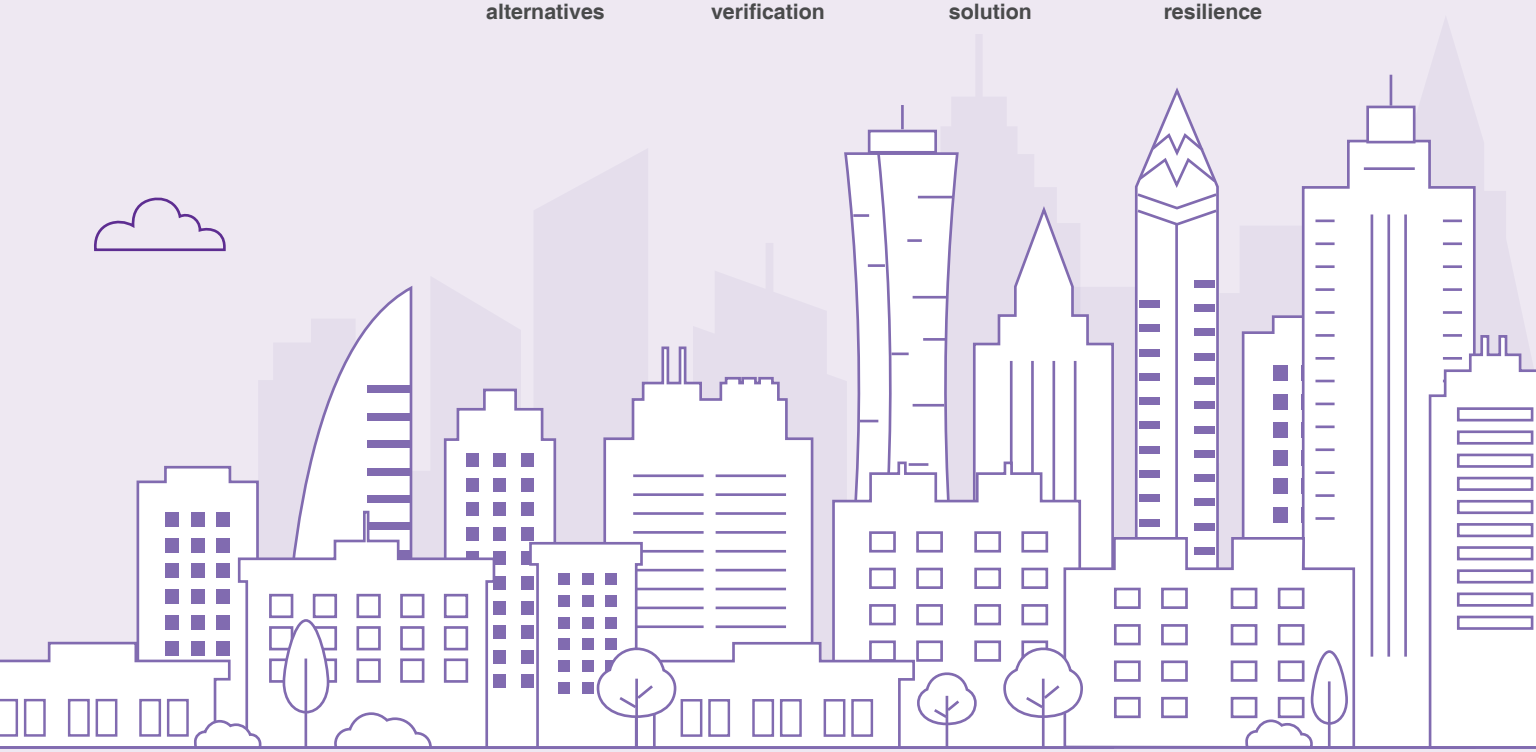
Proportionality

Less intrusive alternatives

Risk based verification

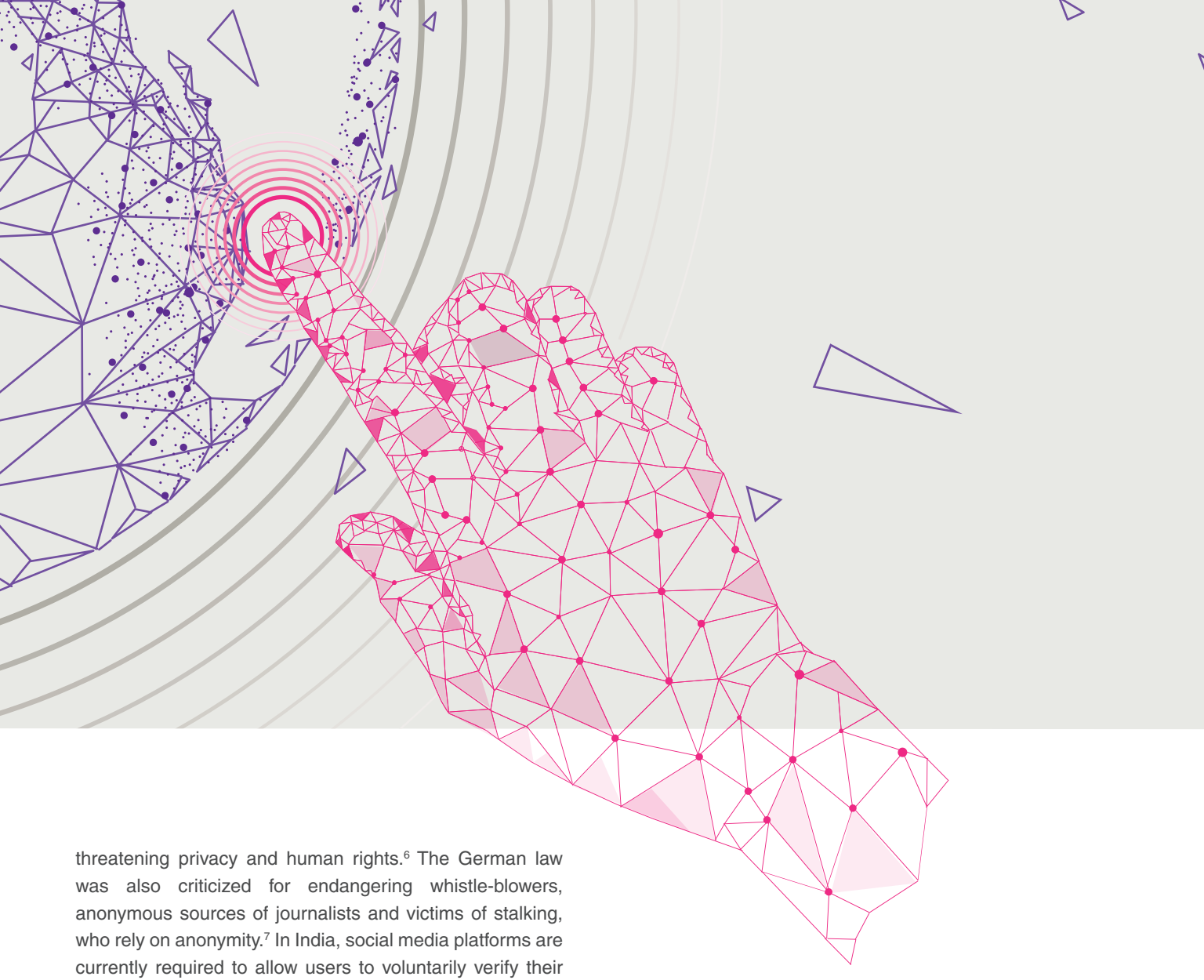
India specific solution

Building resilience

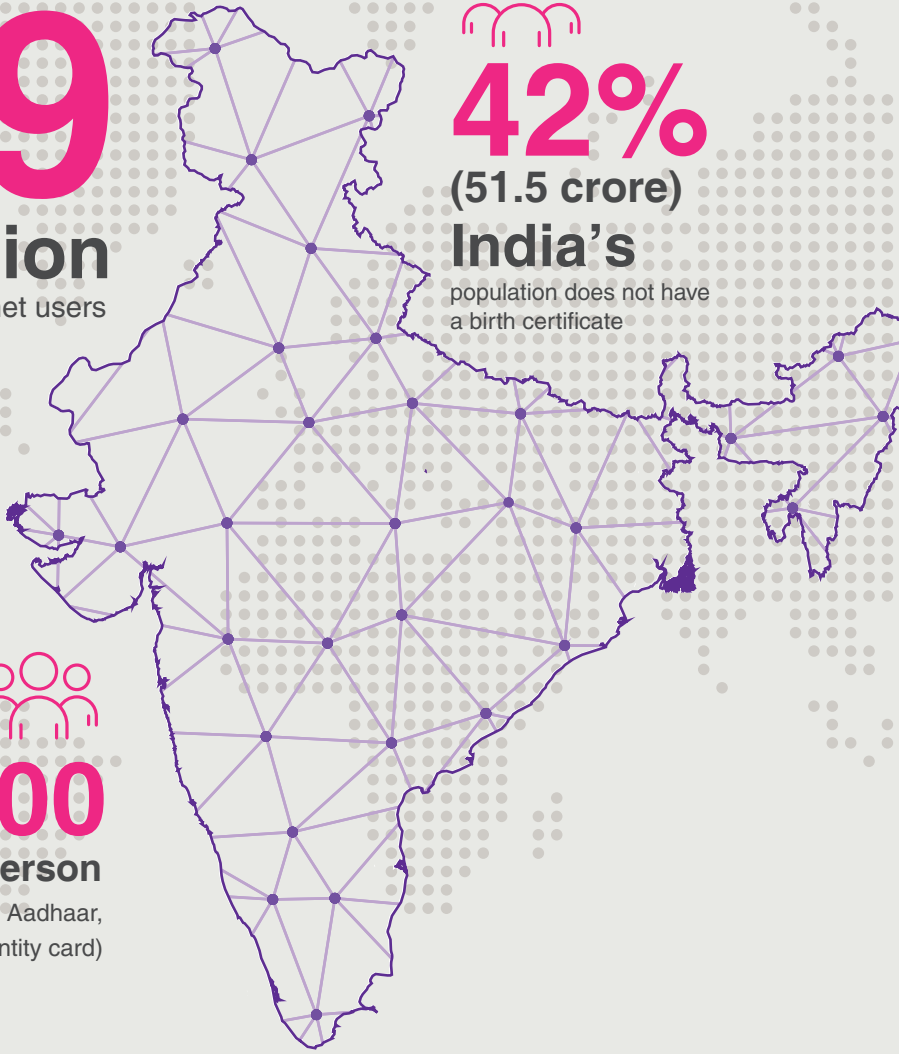


Chapter I: Introduction

Increasing instances of online harms have prompted law and policy makers to assess how to better identify and trace perpetrators on the internet, who often hide behind fake or anonymous profiles.[1] While most online platforms require you to provide a name and an email address, it is difficult to verify if the information provided is indeed correct. This has prompted governments across the world to consider introducing online user verification requirements, to verify if people are who they say they are.[2] For instance, to protect users against digital violence and anonymous hate speech, Germany has proposed a law that requires platform operators to disclose IP addresses of users.[3] In 2023, Vietnam proposed a law that would mandate real identity registration for social media accounts to combat online scams.[4] However, verification requirements are criticised for diluting the degree of anonymity afforded by the internet, which is considered crucial for freedom of speech and expression and democratic discourse. In fact, the proposed Vietnamese law has been condemned for curbing political speech[5] and



threatening privacy and human rights.[6] The German law was also criticized for endangering whistle-blowers, anonymous sources of journalists and victims of stalking, who rely on anonymity.[7] In India, social media platforms are currently required to allow users to voluntarily verify their accounts, such as through a mobile number.[8] However, as mandatory verification become more prevalent, it is necessary to assess, for the Indian context, to what degree should user verification mandates be imposed on social media websites.



759
million
active internet users

42%
(51.5 crore)
India's
population does not have
a birth certificate

₹700-800
per person
(unless done with Aadhaar,
India's national identity card)

With its 759 million active internet users, online user verification in a country like India poses its own infrastructural challenges.[9] User verification is capital and infrastructure intensive. There are massive costs associated with collection, verification and storage of personal data required for user verification. Various estimates show that user verification requirements like KYC cost around INR 700-800 per person (unless done with Aadhaar, India's national identity card).[10] This adds to a huge cost of compliance, given the scale at which social media companies operate. This would be over and above the costs associated with building the infrastructure, deploying manpower and storing the data safely. User verification will drive up the customer acquisition cost and also lead to customer drop off.

These costs can be prohibitive for smaller players and act as a barrier to entry in the digital ecosystem, thereby hindering their innovation and growth in the long run. Substantive regulatory costs due to complex regulatory regimes have a detrimental impact on the growth of businesses, often forcing them to shut their operations. For instance, a fragmented and complex regulatory environment is often cited as a reason for the lack of successful home-grown digital businesses in the European Union.[11] The live streaming content service Twitch's exit from South Korea is attributed to the country's prohibitive network fees in comparison to other countries.[12] A 2022 study by consumer trust society CUTS International, also highlighted the numerous compliances within the Indian digital ecosystem that disproportionately impact India's digital businesses and start-ups.[13] It underscored that, as of 2020, an average Indian business has to comply with 25,537 central compliances. These become 69,233 compliances if the company operates in all states,[14] running contrary to India's aim of promoting ease of doing business.[15] Such costs impact the digital economy and ultimately India's goal of becoming a 5 trillion USD economy.

Safeguarding the data of millions of users is also a humongous task. Platforms will either have to rely on government infrastructure (which comes with its own issues of surveillance and vulnerability) or build their own robust digital architecture to safely collect and store data of millions of users. Platforms will thus become even more susceptible to cybersecurity breaches and data leaks.

User verification also must be seen in the context of India's demographic. A majority of India's population, particularly from marginalised communities, are reported to not have valid identification documents.[16] As per reports, at least 42% (51.5 crore) of India's population does not have a birth certificate.[17] Although

the UIDAI website suggests that 99% of Indians have an Aadhaar card, it is not considered proof of age. Mandating the submission of identity documents, to access online platforms, creates access barriers to social media and the internet, further alienating these communities. Thus strict user verification will also adversely affect India's goals under the Digital India mission to transform into a digitally empowered society and economy.

Online verification requirements can range from a simple captcha requirement to verify if you are human, age verification, to strict measures such as complete identity verification. Implementation of strict identity verification requirements in the interest of national security or public safety poses threats to fundamental rights of citizens, specifically their right to privacy and free speech. However, the right to privacy is not absolute. And can be restricted on certain grounds such as security of the state or public order. Thus, the challenge for policymakers in India is to balance the liberty of citizens and national security, while also ensuring that digital innovation in India is not negatively impacted.

This white paper explores whether and to what degree should user verification requirements be imposed on social media platforms.

User verification requirements on the internet

Chapter I

Lays down the background of the debate.

Chapter II

Discusses the relationship between anonymity and user identification and the benefits and risks associated with online anonymity. It emphasises the need for preserving a certain degree of anonymity when implementing user verification measures.

Chapter III

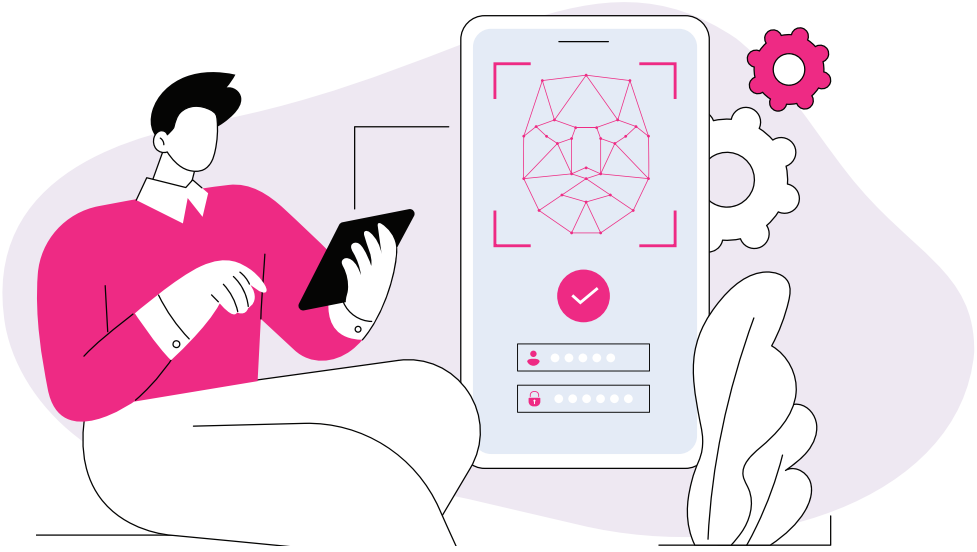
Discusses reasons for introducing user verification requirements in the financial and telecom sectors. It argues that identical requirements should not be imposed on social media platforms, because of the difference in the nature of services, risks and trade-off of rights.

Chapter IV

Examines user verification mandates in other jurisdictions, namely, South Korea, Brazil, the United Kingdom and the European Union. It highlights the various challenges and criticisms surrounding them, any perceived benefits and other consequences in these jurisdictions.

Chapter V

Provides the principles to be followed while considering user verification requirements on social media platforms in India.



Chapter II:

Exploring user verification and anonymity

This chapter discusses the differences between user identification, verification and authentication on the internet. It explores the relationship between user verification and anonymity. It discusses anonymity as a concept, and its positive and negative use cases. It explores how user verification dilutes online anonymity and the various benefits it offers. In doing so, it argues that user verification requirements must not completely strip away anonymity and some degree of online anonymity must be preserved to protect free speech and privacy of users.

A. Understanding identification, verification and authentication

'Identity' is a collection of traits, indicators or characteristics that offer themselves as points of distinction between individuals.[18] Identification thus happens through 'identifiers' i.e., the pieces of information, which individually or together help in distinguishing one individual from another.[19] This may include a person's name, age, date of birth, etc. These are generally referred to as real world identifiers. However, real world identifiers are not the only types of identifiers. There may also be identifiers assigned to people for purposes of communication.[20] For instance, assigning a customer number to a person for interaction with a sales company or an online user's IP address.

The terms identification, verification, and authentication are often used interchangeably. However, they differ in

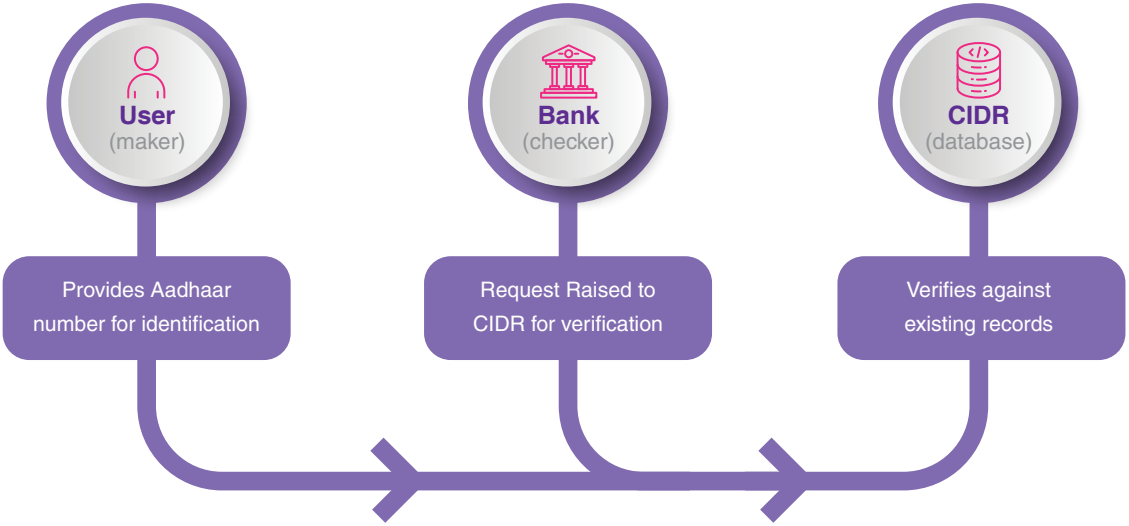
meaning. Identification generally involves self-declaration of information without a third party verifying that information. For instance, asking users to provide their name to register on a social media platform. On the other hand, verification means determining the veracity of the details or documents provided. Authentication means ensuring that a person is who they claim to be. However, verification and authentication are often understood and used synonymously[21] and this paper also uses them synonymously for ease of understanding of the reader.

Authentication/verification is a two-step process which involves two parties - (1) the person who provides their information/the user (maker) and (2) the organization / person that verifies such information (checker). It involves verification of - (a) identity documents and (b) identity of the person furnishing such documents.

In the first step, the checker verifies the authenticity, validity, and acceptability of identity documents. Acceptability means that the documents can be accepted as per law or the checker's internal policies. Authenticity refers to the legitimacy of the document. Validity means the document does not need to be renewed or has not expired.

In the second step, the checker verifies the identity of the person who furnishes such an identity document. Before online verification became prevalent, a person's identity was verified through in-person verifications. The checker would physically verify the identity document and then verify the identity of the person who furnished the document. For instance, at airports, the airport or airline authorities verify that the identification document submitted is valid and also physically verify that the document belongs to the person providing the identification document (by physically matching the photograph in the ID with the face of the person).

In the online context, for instance, Aadhaar-based authentication is widely used by regulated entities such as banks for verification. Banks will ask users to submit their Aadhaar number. The details provided are submitted to the Central Identities Data Repository (CIDR), a central database which then verifies if the data provided matches the information available with it.[22]



B. Unpacking anonymity

The next section explores how user verification impacts online anonymity. It discusses the concept of anonymity, its importance and how it can be misused in certain cases. It then explores how online user verification requirements dilutes anonymity, and thus endangers the various rights it enables.

What is anonymity?

Anonymity is the lack of distinguishing characteristics or 'remaining nameless.'[23] In anonymous interactions, individuals conduct their interactions without sharing identifiable attributes or characteristics.[24] For instance, VPN service providers allow users to browse the internet with some degree of anonymity.

Anonymity is the opposite of identifiability, where it is not possible to recognise an individual.[25]

It is, thus, the condition of avoiding identification.[26] It is because of this that anonymity allows bad actors to hide in plain sight.[27]

There are different degrees of anonymity

1 Complete anonymity

'Complete anonymity' is where the individual cannot be traced at all given the details shared by them.

2 Partial anonymity

'Partial anonymity' allows for a limited tracing of an individual; it captures certain distinguishable traits which present a picture of the individual, such as their gender, geographical location etc.

3 Non-anonymity[28]

'Non-anonymity' is where an individual is easily identifiable based on the traits shared by them in an interaction.[29]

For example, a visa application requires persons to provide identity documents such as their passport.

Online anonymity is also different from offline anonymity. Offline anonymity could be achieved by using masks, not revealing one's name, having a secret ballot, among other things.[30] However, merely concealing your name is not enough to preserve anonymity on the internet.[31] Online platforms by default collect various 'identifiers', such as IP addresses or cookie data, which can lead to tracing the user.[32]

Complete online anonymity makes it difficult to identify people on the internet. With the increase in online offences, governments are debating between the need to preserve online anonymity versus introducing requirements to verify identity of online users. However, proponents for anonymity argue that some degree of anonymity is justified based on the wide benefits it provides for people and society, especially when it comes to having a thriving democracy.[33] Thus, the debate is, to what extent should online user verification requirements strip away anonymity.

Anonymity as an enabler of rights - Positive use cases of anonymity

The Report of Special Rapporteur on the promotion and protection of right to freedom of opinion and expression (Special Rapporteur Report) recognizes anonymity as an enabler of the right to privacy and freedom of speech and expression.[34] In Justice K S Puttaswamy (Retd) v. Union of India (2017), Justice Chandrachud noted academician

Alan Westin's theory of privacy which recognizes anonymity as one of the states of privacy; where an "individual seeks freedom from identification despite being in a public space".[35]

Online anonymity allows people to express themselves freely, engage in criticism and political satire,[36] voice unpopular or contrarian beliefs without fear of punishment or retaliation.[37] This freedom to disagree and criticise the state is fundamental for a deliberative democracy.[38] For instance, human rights activists need anonymity to speak out against a hostile state.[39] Thus, it allows for political dissent, which is particularly important in environments where free speech is restricted or where dissenting opinions may be met with repression.[40] Encryption and VPNs are important identity-concealers that aid political organization.[41]

For instance, in 2019, pro-democracy protestors in Hong Kong used encrypted applications to organize protests and disseminate crucial information. Online anonymity protected them from surveillance by Chinese authorities. If not for anonymity enabling applications, protestors could be subjected to potential retribution by authorities.[42]

Anonymity also promotes freedom of the press, by helping them protect their sources.[43] It helps protect journalists and whistle-blowers, who can reveal crucial public interest information, without fear of identification.[44] There are several examples of this:

Wael Ghonim, an activist, used an anonymous Facebook page "We are all Khaled Said", to expose government suppression and mobilise protests against corruption and police brutality in Egypt.[45]

Figure 1: The event invitation to Egypt's revolution on the 'We Are All Khaled Said' page.

Anonymity also allows sharing of anonymous tips and reports with law enforcement agencies,[46] particularly, in cases where individuals fear retaliation or have concerns about their safety if their identity is revealed.[47] Some jurisdictions, such as India, have anonymous crime reporting systems in place.[48]

Anonymity also helps in destigmatization. It enables conversations on topics that are regarded as taboo, for instance, sexuality, sex education, sexual abuse, illness, homosexual marriage,[49] sexual orientation or religion.[50] Anonymous identities can enable marginalized groups access information, social services, communities and spread awareness of issues they face, while maintaining their safety. For instance, many platforms for reporting gender-based violence in India, such as Red Dot Foundation's platform, Safecity[51] and howrevealing.com, allow users to report anonymously. Anonymous reporting only highlights the egregiousness of the harm instead of focusing on the identity of the victim or the perpetrator, both of which create bias.[52]

The benefits of anonymity have also been recognized by the law in India. The Whistle-blower Protection Act 2014[53] protects whistle-blowers by mandating their identity to remain concealed.

Laws related to sexual offences criminalize unintended disclosure of victim's identities to protect victims. For instance,

Bharatiya Nyaya Sanhita 2023 (which replaced the Indian Penal Code 1860) criminalises the disclosure of the identity of victims of sexual offences.[54]

The Protection of Children from Sexual Offences Act 2012 also prohibits the media from disclosing information such as name, address, photograph, family details, school, neighbourhood which could lead to disclosure of the identity of a victim.[55]

The HIV and AIDS (Prevention and Control) Act, 2017 protects anonymity of HIV-positive persons during court proceedings and prevents publishing of information that may lead to their disclosure.[56]

Another positive use case of anonymity is in research studies and surveys, where participants are often given the option to remain anonymous. This encourages honest responses, particularly for sensitive topics where individuals may be reluctant to share personal information if they cannot do so anonymously. Anonymity in research can lead to more accurate data and insights.[57]

Despite multiple benefits, malicious actors sometimes misuse online anonymity for nefarious purposes. Some instances are discussed below.

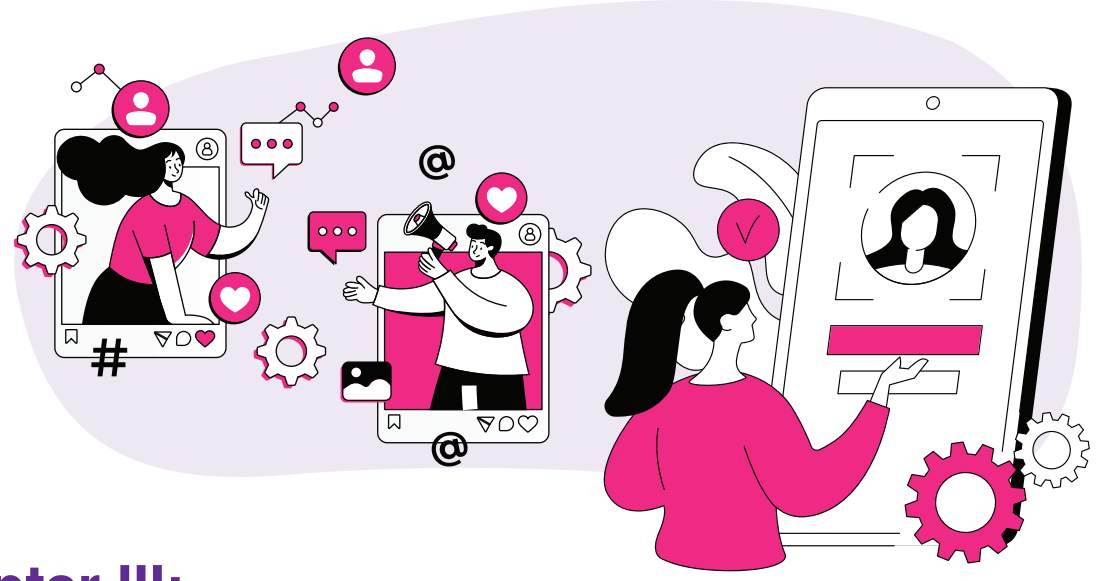
Misuse of online anonymity

While online anonymity promotes a robust deliberative democracy, opponents argue that it promotes harmful behaviour and decreases accountability.

They argue that anonymity promotes behaviour that falls below established standards of civility[58] due to the supposed lack of consequences.[59] Because it becomes easier to indulge in harmful behaviour when it is not dictated by norms of civility, courtesy and decency.[60] It is argued that anonymity leads to 'deindividuation', that is, lowering of social inhibitions and a state of loss of self-awareness.[61] People who know they are anonymous may feel disassociated from their identity and ignore the consequences of their actions.[62] It is also contended that online anonymity makes it difficult to identify and apprehend perpetrators of crime on the internet.[63] Law enforcement agencies argue that it becomes difficult to track criminals without knowing who is behind an online pseudonym or anonymous account, making investigation of offences difficult.[64] Greater resources and specialized technical knowledge is needed to then trace and apprehend such individuals.[65]

User verification dilutes anonymity

There is a constant tussle between balancing the benefits and risks associated with online anonymity. Verification and anonymity lie on opposite ends of the spectrum. Higher degree of verification results in greater dilution of anonymity. For instance, using a social media platform may require a user to share their email ID, which adds a layer of identifiability to their online presence. Whereas using online banking services would require additional layers of identifiability such as location, mobile number, answering security questions etc., thereby further peeling away anonymity. Stripping away anonymity erodes the benefits it offers, including threatening a person's freedom of speech and right to privacy. Thus, user verifications requirements must dilute anonymity only to the extent necessary to the objective they seek to achieve. Some degree of anonymity must be maintained, in order to protect privacy and free speech of users.



Chapter III:
Evaluating the need for user verification measures on social media platforms

This chapter discusses user verification requirements in the financial and the telecom sectors - reasons for their introduction and harms they seek to address. It juxtaposes these mandates against identification and verification requirements on social media platforms. It then makes a case for having different degrees of user identification or verification for different types of services. This is attributable to differences in the nature of services offered by these sectors, degree and propensity of risks and harms, and the differential impacts on user rights. It argues that user verification requirements on social media must pass the constitutional standards for proportionality. It also discusses the less intrusive measures available, which maintain some degree of anonymity, but allow for identifying bad actors if required.

A. User Identity verification in the financial sector

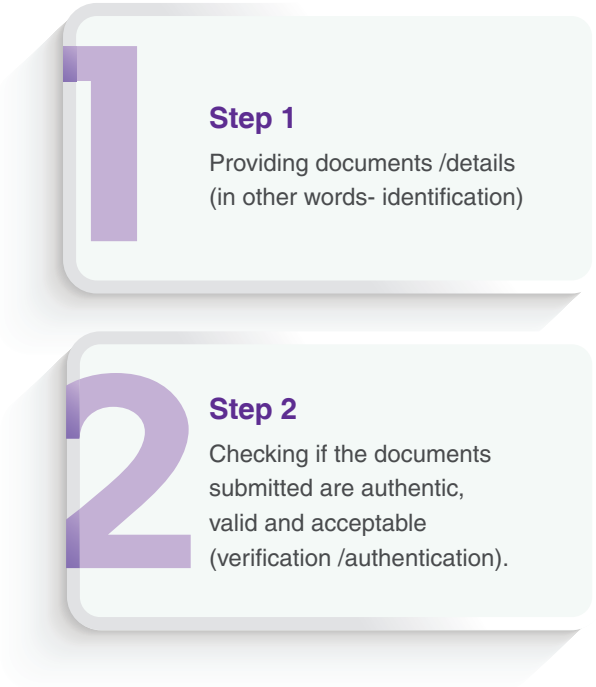
User verification was first introduced in the financial sector, to combat money laundering and terrorist financing. The Financial Action Task Force (FATF), the global organization for combating financial crime, recommended undertaking thorough customer due diligence through Know-Your-Customer (KYC) norms, and prohibited the creation of anonymous or accounts under fictitious names.[66] The FATF recommendations provide a baseline requirement for financial institutions to collect data such as customer name, identity proof, address proof etc., but allow countries to adopt higher and more stringent standards for customer due diligence.

In India, the obligation to conduct customer KYC flows from the Prevention of Money Laundering Act 2022 (PMLA) and rules/regulations under it. Under the PMLA, reporting entities (RE) (such as banks, financial institutions, insurers) are required to verify the identity of clients through online or offline verification, against government issued Aadhaar cards or other officially valid documents such as passports, driving licenses. The RE is required to identify and verify the identity of their customers, at the time of opening the customer's account, for international money transfers and for domestic transactions over a certain limit.[67]

The Reserve Bank of India has also come out with KYC directions where REs such as banks, must conduct customer due diligence when the customer opens an account[68] or undertakes transactions such as deposits, withdrawals, or transfer of funds or applying for a loan.[69] The customer is required to submit identification documents such as passport or driving licence, Aadhaar number or proof of possession of Aadhaar number or Permanent Account Number.[70]

Certain sectoral regulators also impose KYC norms- for instance, the Insurance Regulatory and Development Authority of India (IRDAI) requires insurers to conduct KYC of their customers[71] and SEBI requires KYC of investors investing in the stock markets in India.[72]

The KYC broadly involves two steps



For instance, in biometric Aadhaar e-KYC, the user submits their biometric information (iris or fingerprint data),[73] which is matched against the biometric information of the user as stored in the CIDR database.[74] Offline Aadhaar KYC requires users to upload a live photo which is matched against existing records.[75]

Thus, there are strict user verification norms in the financial sector in India to combat financial crimes such as money laundering, terrorist financing, fraud etc.[76] and ensure the integrity and stability of the financial system.

B. User Identity Verification in the Telecom sector

Telecommunication services are integrated with many financial transactions such as banking and trading. Phone numbers are also extensively used for authentication. One-time Passwords (OTPs) are sent to phone numbers to verify users. Many perpetrators use fake telecom connections to conceal their identity. User verification requirements have thus been introduced in the telecom sector to combat SIM fraud, phishing, and financial fraud.

Telecom service providers (TSPs), such as Airtel, Reliance Jio etc. are required to verify the identity of customers when they're purchasing SIM cards or landline connections.[77] TSPs collect details such as name, address, nationality, bank details, among other things, through customer acquisition forms as well as other identification documents, including Aadhaar number and photographs, to verify the identity of the subscriber.[78] TSPs are also required to preserve call detail records and IP details of the users for scrutiny by the Government.[79]

Further, the recently passed Telecommunications Act, 2023 (Telecom Act) that overhauls the regulation of telecommunication services in India also imposes user verification requirements.

TSPs are obligated to identify their customers through any 'verifiable biometric based-identification' methods that will be prescribed by the Central Government.[80] Concerns have been raised over the privacy implication of this measure.[81] The multiple instances of data breaches being reported such as the CoWin data leak[82] or the ICMR data breach[83] have also exposed the vulnerability of India's security infrastructure for sensitive personal data. Thus, there are also concerns over the security of the biometric data collected and stored by TSPs.

C. User verification on social media platforms

Verification requirements, which were traditionally imposed in other sectors, are making their way to social media platforms, such as age verification, identification of the first sender of messages, data retention requirements, among others. We discuss some of the user verification requirements on social media below, including the concerns surrounding them.

Identifying the first originator of information

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules 2021) require identification of the first originator of information. Significant Social Media Intermediates (SSMIs) i.e., platforms with 50 lakhs users or more which primarily allow users to interact and share information, can be ordered to enable the identification of the first originator of a piece of content (such as a message) on their computer resources, by a court or a competent authority under Section 69 of the Information Technology Act (IT Act).[84]

There have been several concerns surrounding this provision since it was introduced, such as – it compromises the right to privacy and free speech of users by stripping their anonymity on the internet;[85] enabling traceability can weaken encryption on a platform[86] which disproportionately impacts all users; users become prone to increased malicious attacks due to weak security architecture.[87] This provision was also challenged by WhatsApp and its parent company Facebook (now Meta),[88] which is currently pending adjudication.

Experts also agree that the traceability requirement will break end to end encryption (E2EE),[89] which is considered essential to ensure security and confidentiality of all forms of communication over the internet. The 'right to encrypt' is also argued to be a part of the 'right to privacy'.[90] It has also been argued that the traceability requirement does not meet the test of proportionality under constitutional law,[91] and thus is not a reasonable restriction to the right to privacy.[92] However, interestingly, the government has issued a statement that this provision does not violate privacy of citizens and the issue of breaking E2EE is misplaced.[93]

There are also various technical challenges associated with this requirement. The IT Rules 2021 do not prescribe any mechanism to identify the first originator and no conclusive mechanism has been developed yet. Interestingly, the Government in its earlier statement had put the onus of finding a solution on entities like WhatsApp.[94]

Most of the methods that have been proposed till now fail to correctly identify the first originator. For instance, one proposed method involves assigning unique hash values to messages[95] but experts argue this could lead to identification of all users, exceeding the provision's scope.[96] Another suggestion involves tagging the originator's information to messages,[97] but this method also fails to conclusively identify the first originator. This could potentially lead to law enforcement agencies identifying the wrong person.[98] Additionally, if the originator is outside India, the first recipient within India is considered the first originator. Thus, one can easily escape identification by using a foreign number.[99] Further, technological solutions seem to be limited to identifying phone numbers or email addresses, not actual individuals.[100] Further, the platform is only required to identify the first originator on their own network[101] and the provision does not account for cross-posting.[102] Thus, the absolute originator of the content cannot be conclusively identified.[103]

Another concern is the cost associated with building a digital architecture that can enable traceability of the first originator.

For instance, for platforms with 75 million users, the costs can amount to USD 180,000 and for platforms with 750 million users, costs can amount to USD 1.5 million.[104]

These costs can be prohibitive for smaller players and hinder their innovation and growth in the market.

Thus, while the traceability requirement was introduced with an intention to apprehend persons who initiate crimes, such as hate speech or post CSAM content,[105] it has led to widespread concerns over privacy and free speech. It has also been invoked for frivolous reasons. For instance, WhatsApp was directed by a court to identify the first originator of a message about the fake resignation of the Chief Justice of a High Court. WhatsApp was constrained to appeal the order, which was struck down on the ground that the content did not constitute a threat to public order.[106]

Sec. 66A of the IT Act is another example of how a well-intentioned provision led to unintended consequences. Section 66A was introduced to curb online harassment. It penalised a person for offensive, menacing, misleading content or content that causes annoyance over the internet. However, the provision became a tool to silence dissent and file frivolous complaints against citizens.[107] It was

infamously used to arrest a woman for criticising, on Facebook, a citywide shutdown over a politician's death. Another girl who merely liked the post was also arrested. The provision was struck down by the Supreme Court of India for unconstitutionally restricting the freedom of speech and expression, however it continues to be misused.[108]

Another prime example is that of South Korea's real name policy, which required people to mandatorily use their real names online when commenting on news sites[109] or signing up for a website.[110] It was introduced to curb online harms.[111] However, as per studies, the policy actually led to an increase in hacking incidents involving users' identification details and did not actually lead to reduction in online harms.[112] The policy was eventually struck down for being unconstitutional.[113]

CERT-In directions- Data retention requirements for VPNs

Data retention requirements generally require entities to maintain a record of user data and activity. Law enforcement agencies and courts can call upon such entities to provide such information in furtherance of an investigation or proceedings before the court.[114] Data retention requirements, thus, help in connecting acts to actors and promote accountability. However, they may potentially threaten a person's right to privacy and anonymity in some cases.[115] For instance, in India, such data retention requirements also apply to VPNs.

The 2022 directions issued by the Indian Computer Emergency Response Team (CERT-In Directions), require entities, including data centres, cloud service providers and VPN service providers, to store customer information such as validated name, email address, IP address, validated address, contact numbers and ownership patterns of subscribers.[116]

VPN service providers are important tools for users to access the internet anonymously, exercise control over their personal data and prevent involuntary sharing of identity with third parties.[117] They are important tools for protecting the right to privacy.[118] Many VPN service providers have hence expressed concerns about the impact of these requirements on users.[119] Certain international VPN service providers have also suspended their India operations due to the extensive storage requirements.[120] SnT Hostings, an Indian VPN service provider challenged the CERT-In Directions before the Delhi High Court, arguing that it violated the test of proportionality, storage limitation, purpose limitation and undermined privacy.[121] The CERT-In, on the other hand, argued that the total anonymity of VPN can be misused by users.[122]

India enacted its data law i.e. the Digital Personal Data Protection Act (DPDPA) on 11 August 2023.[123] The DPDPA places certain obligations on data fiduciaries i.e., the entities that determine the purpose and means of processing personal data.[124]

For processing personal data of children (persons below 18 years) and persons with disabilities, data fiduciaries are required to obtain 'verifiable' consent of the parent or lawful guardian.[125] The DPDPA does not specify what constitutes 'verifiable consent'. The manner of collecting verifiable consent will be prescribed through rules. There have been wide ranging concerns over this requirement.[126]

In order to obtain verifiable consent of the parent or lawful guardian, the data fiduciary will have to conduct verification at multiple levels. It will have to verify the age of the person claiming to be the parent (to ensure the person is not under age), the relationship between the child and the parent (to verify the person is the parent) as well as verify the identity of the parent itself. It may have to authenticate documents to verify details such as age and identity of the parent.

For instance, Z, a 17-year-old, tries to make an account on a social media platform by declaring his age as 18 years old. The social media platform will need to have a robust mechanism to verify Z's correct age, such as through official documents. Thus, it will have to ask all users to provide identification documents. In another instance, Y wants to make an account for her 13-year child on a social media platform. The social media platform will have to not only verify Y's identity but also confirm that she is the parent.

Thus, the data fiduciary will be mandated to de facto verify the identity and age of all users on its platform to implement this requirement. This excessive collection of personal data goes against the principles of data minimisation where entities are expected to collect the minimum amount of personal data needed to provide a service. Storing the personal data of millions of internet users also poses the risk of cybersecurity incidents, leaving the data susceptible to leaks.[127]

The government had earlier considered an e-KYC based model for verification under the DPDPA.[128] The model considered using identity verification documents to verify the age of users. However, experts argued that this will lead to excessive sharing of KYC documents such as Aadhaar cards with private entities, thereby posing a security risk.[129] They also claimed that the feasibility and reliability of this model is low.[130]

As per reports, the government is considering multiple modes of verification under the rules- one, that utilizes public infrastructure and government authorized entities to verify identity through electronic tokens such as the DigiLocker system or using other reliable details of identity and age available with the platform.[131] Social media platforms will need to build technical infrastructure to carry out this verification requirement as well as maintain security of this data.

D. To what degree should user verifications be imposed on social media platforms

User verification is not a one size fits all solution. Different types of services require different approaches based on a variety of factors such as- the nature of service, degree of risk, propensity of harms, economic and technical feasibility, privacy expectations of the users, the trade-off of rights, among others.

Social media platforms are avenues for speech and social connection, unlike for instance, entities in the financial services. They perform the important function of helping deliberative democracy thrive, foster freedom of speech and expression, and allow users to express their authentic selves without fear of repercussions.

Thus, the trade-off in introducing strict user verification requirements on social media platforms is much higher. Strict user verification requirements on social media platforms will disproportionately impact a user's fundamental rights. It will have a chilling effect on free speech that ultimately curbs the benefits that anonymity offers.[132]

Since mandatory user verification requirements encroach upon a person's right to privacy, it must pass constitutional standards of proportionality.[133] The test of proportionality requires a state action to fulfil the following criteria:

User verification requirements must only be imposed on social media platforms to the extent necessary to the objective being sought to achieve and relevant to the use case. The measure should pass the test of 'necessity'. So, if the objective is to verify age, then complete identity verification is not necessary. For instance, under the DPDPA, the objective is to ensure online safety of children (or to restrict certain content to children). However, mechanisms such as- requiring identity documents to verify identity of parents will lead to de facto identification of all users of the platform.

The unintended consequences of the measure should also be carefully considered. Law makers should consider empirical data on whether the requirement will meet its intended objective or lead to more harms.

The impact on users' rights should be proportionate to the intended objective. For instance, the traceability requirement is argued as disproportionate, since it compromises the privacy of all users on a platform to identify certain bad actors[135] and may even lead to innocent individuals being identified as first originators.[136]

In case of user verification, the question to ask is- Is the risk to user's privacy proportionate to the problem being sought to be solved?

This also means that the least intrusive measure or alternative should be adopted. User verification requirements are not the only mechanism to identify people on the internet. There are technical alternatives that offer a middle ground between maintaining some degree of anonymity but still making it possible to identify perpetrators, if needed. The alternatives aim to balance security while minimizing concerns surrounding strict user-verification requirements. Pertinently, these alternatives require users to prove that they are indeed the right person to be accessing a service, without requiring them to establish their individual identity.

Some of these models are discussed below:

Information already available with social media platforms:

Most online services already collect metadata i.e. the data that describes a piece of information.[137] This could include details such as- which users send messages to each other, when these messages are sent, size of these messages[138] and location from where messages are sent, among other details.[139] Law enforcement agencies have acknowledged that metadata can provide comprehensive information about user activity and the networks they form part of. Therefore, meta data collected by social media websites can be used for the detection and investigation of online offences.[140]

Online platforms also collect mobile numbers, IP addresses, cookie data, device and network information of users. Thus, while users may be anonymous to each other, online platforms generally have enough information to track users if needed.[141] IP addresses are numerical labels assigned to each device connected to a computer network that uses the internet protocol for communication.[142] An IP address can provide information about a user's general location and internet service provider, without revealing the person's identity.[143] IP addresses have therefore been considered to be sufficient to collect information about users and identify them.[144] For example, an IP address can help identify a person's approximate location such as the

state, city or the pin code of the place. Although time-consuming, law enforcement agencies have successfully been able to track origins of cyber-crimes using IP addresses.[145] Further, law enforcement can get details such as, the name, address and bank details from TSPs who are already required to collect such data.[146] Requiring social platforms to collect and store personal data which is already collected by TSPs will likely not hold against statutorily or judicially recognized standards of data minimization.

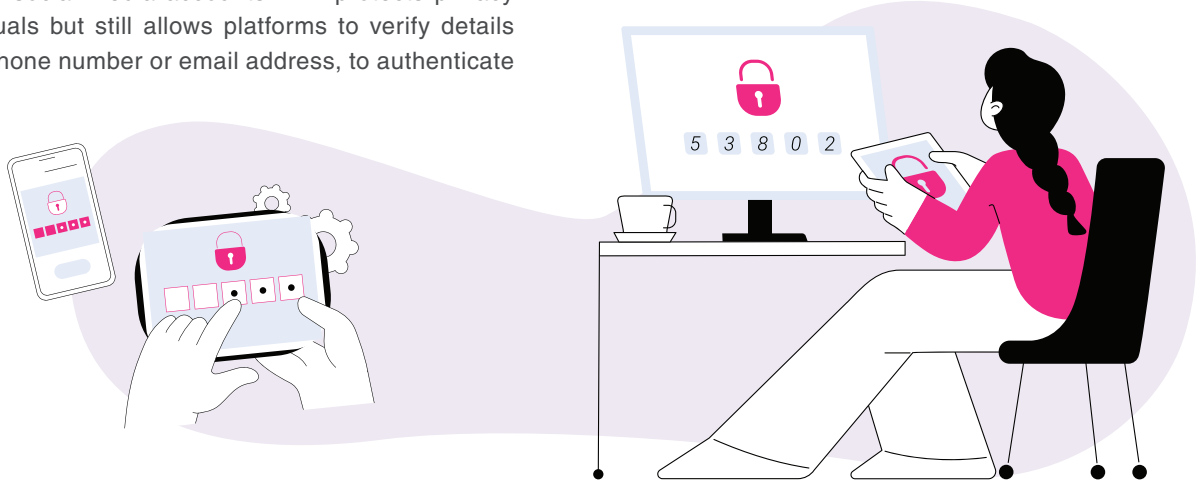
Two-Factor Authentication (2FA):

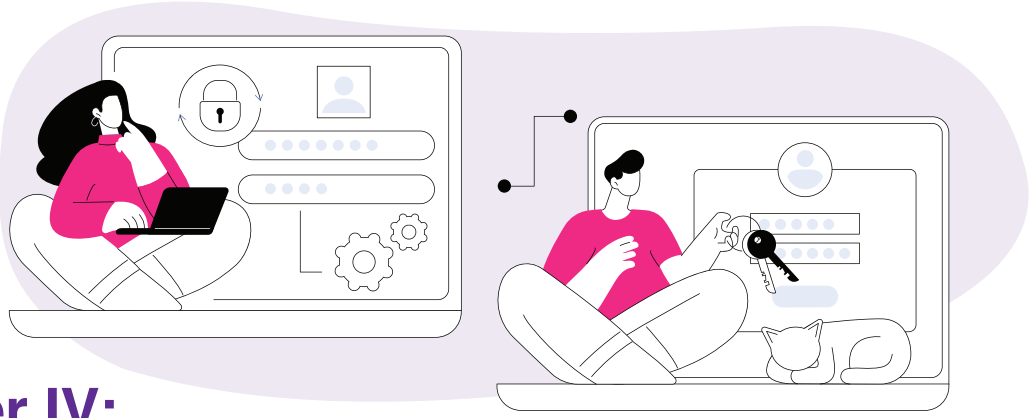
Two-factor authentication is an extra layer of security that helps authenticating the user of an account. Generally, 2FA involves a user establishing her credentials through two consecutive steps.[147] The user will be required to put in their password. After successfully entering the correct password, an OTP will be sent to the user's phone number or email address. Once she enters the correct OTP, the user will be authenticated. Some platforms also use a security question as the second layer of authentication. Similarly, some online services also send a verification link to the user's email address or phone number. 2FA is commonly used while logging into internet banking profiles or social media accounts. 2FA protects privacy of individuals but still allows platforms to verify details such as phone number or email address, to authenticate the user.

Self-Sovereign Identity (SSI):

SSI is a model that helps individuals manage and control their digital identity in a secure, private, and decentralized manner.[148] Users can decide what data is included in their digital identity, who can access it, and for what purposes. This helps protect the privacy and security of individuals' data. Information is typically stored on a blockchain or other distributed ledger technology, ensuring that it is secure and tamper-proof. SSI employs cryptographic techniques, such as digital signatures and decentralized identifiers to ensure the integrity, authenticity, and security of identity data. Verification can be done without revealing more personal information than necessary. SSIs are designed to be interoperable and work across different services, platforms, and applications.[149] Users can use their digital identity to access government services, services of financial institutions and online marketplaces too.[150] For instance, this can be used in cases where only the age has to be verified but not the name or address.

Thus, in many cases, strict user verification may not be the only measure available to achieve the intended objective.





Chapter IV: Exploring user verification in other countries

In this chapter, we will examine the user verification mandates in certain other jurisdictions and highlight the various challenges and criticisms surrounding them, any perceived benefits and other consequences. It examines user verification mandates in South Korea, Brazil, the United Kingdom and the European Union.

A. SOUTH KOREA

South Korea first introduced a real name system in 2004 with an amendment to the Public Official Election Act, which required people to verify their real names before commenting on online news sites during election periods.[151]

In 2007, another law was introduced[152] that required users to mandatorily use their real name online when signing up for websites, in an effort to curb online harms.[153] However, various empirical studies, including one commissioned by the government, found no evidence that illegal activities decreased due to this user verification requirement.[154] Studies showed that instead of promoting internet security, the real name policy actually introduced new hazards. The websites collecting millions of users' identification details became treasure troves for hackers, and the number of hacking incidents reached alarming proportions.[155] In August 2012, the South Korean constitutional court struck down the 2007 provision as unconstitutional, on the ground that it infringed upon the rights to free speech and personal identity.[156] The Court added that there wasn't sufficient evidence to suggest that the real name policy led to a decrease in online harms. The Court also reasoned that there were alternatives available- the authorities could track people through IP addresses and websites had other means such as blocking or deleting malicious posts.[157]

Thereafter in 2021, the provision in the Public Official Election Act was also struck down by the court as unconstitutional.[158] The court emphasized that prioritizing administrative convenience over freedom of expression unduly limits anonymous expression. The court further observed that the requirement was based on a vague premise that illegal content might reduce under the real-name internet system.[159]

B. BRAZIL

The "Marco Civil da Internet" or the Internet Bill of Rights[160] provides for freedom of expression but prohibits online anonymity.[161]

However, there have been instances where courts have defended anonymous speech on the basis of free expression and privacy.

In a significant ruling, a ban on the 'Secret' app, which allowed users to comment anonymously, was overturned by a Brazil civil court. The court noted that though the app allowed relative anonymity, it was possible to identify users if needed, such as through IP addresses.[162]

Hence, the Brazilian court seemed to have differentiated between absolute anonymity and relative anonymity. Brazil also does not have restrictions on VPNs and anonymity browsers.[163]

However, legislative proposals for user verification have been considered. In 2020, the Brazilian Senate approved a draft "Fake News Bill", which had a mandatory identification requirement through a National ID and mobile number, for social media and private messaging services.[164] The requirement was criticised for violating privacy rights.[165] Amid the criticism, a revised draft was introduced[166] where identification requirement is not mandatory.[167] The bill is yet to be approved into law.

C. UNITED KINGDOM (UK)

The UK does not have a real name policy, however recently introduced an age-gating requirement. In October 2023, the UK enacted the Online Safety Act (OSA), a landmark legislation regulating the internet.[168] The OSA casts a duty on online platforms to prevent children from accessing harmful content, by ensuring age assurance (either age verification or age estimation or both).[169]

Age verification means a measure adopted to verify the exact age of users,[170] while age estimation refers to a measure adopted to estimate the age or the age range of users.[171]

The OSA itself does not prescribe a method for conducting this age assurance, as long as the method is highly effective at correctly determining whether a user is a child. The industry and civil society have raised several concerns over the age verifications requirements. They argue that platforms would have to choose between sanitizing their entire platform impacting free speech or forcing all users to verify their age, impacting privacy.[172]

In December 2023, UK's communication service regulator, Ofcom released draft Guidance on how age assurance can be done for pornographic websites.[173]

The Guidance has been met with concerns over security of the personal data being stored and heightened risks of cybersecurity breaches.

Interestingly, the issue of ID verification for social media was taken up when the Online Safety Bill was being discussed in Parliament. However, the UK Government had then stated that restricting all users' right to anonymity, by introducing compulsory user verification for social media, could disproportionately impact users such as whistle-blowers, journalists' sources and victims of abuse as well as those who do not have ID documents.[174]

D. EUROPEAN UNION (EU)

The EU is an example of a jurisdiction which protects online anonymity, relying on its existing legal frameworks to tackle online offences. For instance, the Digital Services Act (DSA) regulates online platforms and seeks to prevent illegal and harmful online activities. Though there are no user verification requirements, users are allowed to flag harmful online content. Users can also challenge content moderation decisions of social media platforms, in case their content gets removed or restricted.[175] This approach acknowledges the need for accountability and user protection against illegal content while ensuring that user anonymity and freedom of expression are not unreasonably curtailed.

Additionally, courts have displayed their leaning towards protecting anonymity on social media.

The Court of Justice of the European Union has held that users of electronic communication services are entitled to expect their communication and data to be anonymous unless agreed otherwise.[176] In 2022, the German Supreme Court ordered Facebook to allow users to use pseudonyms on its website. Two Facebook users had filed a legal action when Facebook deleted their account for using pseudonyms.[177] The court ruled that Facebook's actions violated the German Telemedia Act that directs service providers to allow the use of their services "anonymously or under a pseudonym", where technically and reasonably possible.[178]

However, some recent attempts have been made by Member States to bring user verification on social media. For instance, Germany's proposed law which requires platform operators to disclose IP addresses of users.[179] It has been criticised for threatening free speech, privacy, non-discrimination and other human rights.[180]

The French Senate has also approved a new legislation in June 2023, aimed at restricting online crimes,[181] which requires social media platforms to implement age verification mechanisms.[182] The French Junior Minister for Children has suggested the potential use of facial recognition and credit cards for age verification.[183] However, experts have argued that while safeguarding children is essential, age verification regulations overlook technological challenges and shift the responsibility to private organizations.[184]

Chapter V: Conclusion and Recommendations

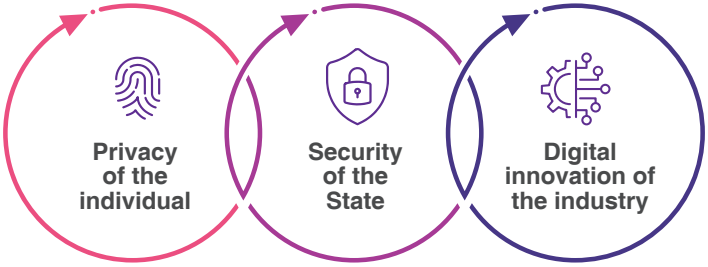
The chapter offers our conclusions and recommendations for implementing user identification and verification on social media platforms in India.

As discussed in the previous chapters, the debate on user verification has multiple facets, which presents unique challenges for policy makers.

There is no single policy or technological solution for this debate. It is no doubt that online anonymity reduces accountability and makes it difficult to identify perpetrators on the internet, which has prompted policymakers and governments to think about having verification requirements on the internet. However, there is a disproportionate trade off in having strict user verification on social media platforms, since it adversely impacts constitutionally protected rights such as privacy, anonymity and free speech. There is also no evidence to suggest that user verification mandates have met intended objectives (such as reducing online harm), in fact global precedent, such as in South Korea, has shown the opposite. There are other alternative measures available which can meet the same objective without compromising on users' fundamental rights.

There are also broader policy considerations for India. The need for a robust digital architecture and resources to safely collect and store data of millions of users; the increased cost of compliances which deters new and smaller players in the market and hinders digital innovation; alienation of Indian citizens who do not have official identity documents. Relying on the State's existing digital public infrastructure solutions, such as Aadhaar, comes with its own constitutional concerns such as violation of right to privacy due to widespread collection of biometric data.

Policy proposals for this debate must balance these interests



We have provided below certain principles that should be kept in mind, when approaching the issue of online verification mechanisms on social media platforms.

Principles for online user verification mandates

User verification requirements must pass the test of proportionality:

Any verification requirement introduced on social media platforms must pass the constitutional standard of proportionality. It must be backed by a law; it should be necessary to achieve its intended objective; the impact of constitutional rights should be proportional to the intended objective; and there should be adequate procedural safeguards to prevent abuse. For instance, strict user verification requirements that prevent users from remaining anonymous online (such as when you are forced to use your real name or forced to submit identity documents) may not be proportionate since they completely strip away anonymity. Identification or verification requirements on social media must retain some partial anonymity, which allows authentication without violating privacy of users.

Use less intrusive measures:

Strict user verification requirements are not the most proportionate solution always as there are other alternatives available. Policy proposals should keep the ultimate objective in mind- the intention is to 'identify' bad actors, and not 'verify' all users on the internet. Here the distinction between identification and verification is crucial. Mechanisms/information that helps identify perpetrators would be a more proportionate solution instead of requiring all users on a platform to reveal their identities and subject themselves to verification. Policymakers should consider the less intrusive alternatives available for authenticating users on the internet or investigating online crimes. This also involves better utilizing the existing mechanisms available. For instance, law enforcement can coordinate with TSPs and platforms to share user account information, which can be combined to trace perpetrators.

Risk based verification:

The verification mechanism should be proportionate to the risk involved. For instance, the kind of user verification needed for visa applications will be different from what is required for opening a social media account. What must be seen is – what is the degree of risk that is to be averted. Thus, the entire spectrum of user verification must be considered – from simple captcha requirements to stringent identity verification. The strictest measures should be imposed only when proportionate. For instance, in case pornography sites want to restrict content to minors, they only need to verify users' age and not their real name or other identity details.

Different scenarios may also merit different responses. Platforms can have in-built algorithms to check suspicious user activity and send prompts for verification only in cases when suspicious activity is detected. For instance, asking users for verification if the platform detects graphic violent content. If an account is reported multiple times for hosting harmful content, then the user of the account can be asked to verify themselves. In some cases, which require a heightened degree of scrutiny, for instance, promotion of financial products such as loans, actors can be asked to get themselves verified.

Develop a unique India specific solution:

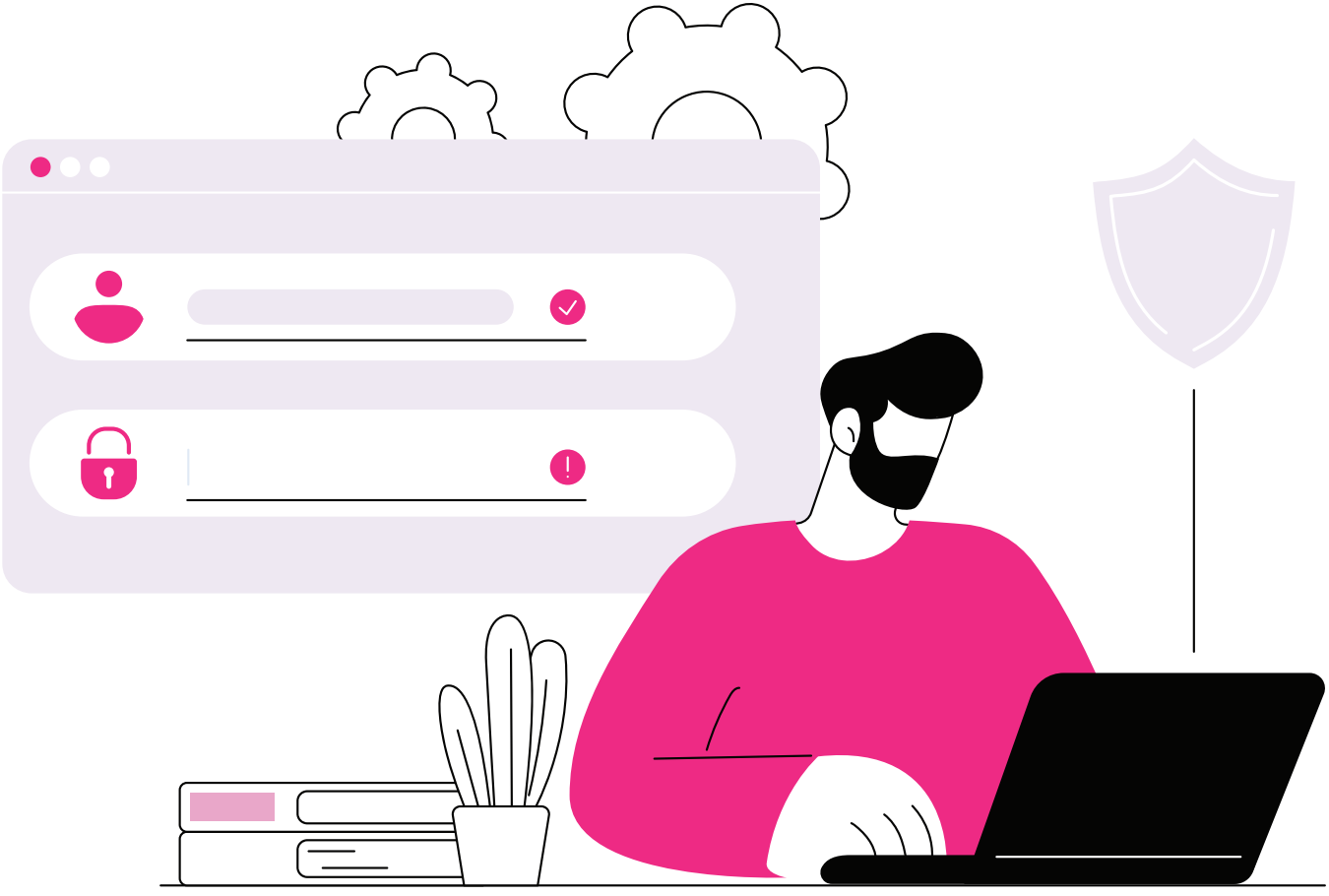
As India stands on the cusp of a great digital revolution, policymakers need to think about solutions specific to India, keeping in mind the country's societal challenges and its growth trajectory into a trillion-dollar economy. The solution must account for India's increasing pool of active internet users, projected to reach 900 million by 2025[185]. It must also consider if the current digital infrastructure is resilient to account for the safe collection and storage of user data. One approach is self-regulation or co-regulation, where platforms can build voluntary codes for improved online safety and user identification. Self-regulation through industry bodies allows for creating an agile and responsive regulatory framework and builds a sense of responsibility and accountability amongst digital players.[186]

Building resilience in the ecosystem:

Policy considerations should also focus on building resilience in the ecosystem, rather than an overtly prescriptive solution. An example of this would be the problem of misinformation on the internet. Earlier solutions were broadly focused on prompt removal. However, there has been a shift, with conversations now focusing on transparency obligations instead. These transparency obligations focus on letting users know that content is AI generated, thereby advising user caution. Similarly, existing laws and a co-regulatory approach with the industry should be used to curb online harms. There should be increased focus on training law enforcement agencies to track pregtors through information that is already collected by social media websites. Investigation efforts can also rely on TSPs who already verify details such as name, address and bank details. Law enforcement should also be trained to exercise their powers in line with procedural safeguards.

Another focus can be on skilling and knowledge building to create awareness among India's internet using populace, especially for children and young adults. As per reports, 66 million Internet users in the country are in the age bracket of 5 to 11 years.[187] Hence, sensitization as part of schools and colleges can also empower children to access social media safely and responsibly.

References



Chapter I: Introduction

[1] Office of Public Affair, US Department of Justice, 'International Statement: End to End Encryption and Public Safety' <https://www.justice.gov/opa/pr/internation- al-statement-end-end-encryption-and-public-safety> (October 2020) accessed 14 February 2024

[2] 'Vietnam's identity verification mandate will violate international human rights' (Access Now, 4 August 2023) < https://www.accessnow.org/press-release/vietnam-social-media-verification/> accessed 14 Februray 2024; Beverly Crawford-Westre, 'Australian government opts against online age verification mandate' (Biometric Update.com, 31 August 2023)<https://www.biometricupdate.com/202308/australian-government-opts-against-online-age-verification-mandate> accessed 14 Februray 2024 Office of Communication, 'Implementing the Online Safety Act: Protecting children from online pornography' <https://www.of- com.org.uk/news-centre/2023/implementing-the-online-safety-act-protecting-children#:~:text=In%20the%20UK%2C%20credit%20card,valid%20to%20the%20issuing%20bank.> (5 December 2023) accessed 14 February 2024;

[3] Alina Clasen, 'Germany Plans Legislation to Block Cyber-Hate Accounts' (www.euractiv.com, 13 April 2023) <https://www.euractiv.com/section/platforms/news/- germany-plans-legislation-to-block-cyber-hate-accounts/> accessed 21 October 202

[4] Sebastian Strangio, 'Vietnam to use Mandatory Identity Verification for Social Media users' (www.diplomat.com, 10 May 2023) <https://thediplo- mat.com/2023/05/vietnam-to-introduce-mandatory-identity-verification-for-social-media-users/> accessed 24 October 2023

[5] Access Now, 'Vietnam's Identity Verification Mandate Will Violate International Human Rights' (Access Now, 16 August 2023) <https://www.accessnow.org/- press-release/vietnam-social-media-verification/#:~:text=As%20Voice%20of%20Vietnam%20reported,and%20foreign%20social%20media%20platforms> accessed 14 February 2024.

[6] Strangio, Sebastian. 'Vietnam to Introduce Mandatory Identity Verification for Social Media Users' (The Diplomat, 10 May 2023) <https://thediplo- mat.com/2023/05/vietnam-to-introduce-mandatory-identity-verification-for-social-media-users/> accessed 14 February 2024

[7] Alina Clasen, 'Germany Plans Legislation to Block Cyber-Hate Accounts' (www.euractiv.com, 13 April 2023) <https://www.euractiv.com/section/platforms/news/- germany-plans-legislation-to-block-cyber-hate-accounts/> accessed 21 October 2023

[8] Rule 4(7), The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

[9] Moneycontrol, Internet users in India set to reach 900 million by 2025: Report, (Moneycontrol, 3 May 2023) <https://www.moneycontrol.com/news/business/inter- net-users-in-india-set-to-reach-900-million-by-2025-report-10522311.html>accessed 21 October 2023.

[10] The HinduBusinessLine, 'Aadhaar brought down KYC cost to 3 from as high as 700, says Nirmala Sitharaman' (The Hindu Business Line, April 15 2023) <https://www.thehindubusinessline.com/economy/aadhaar-brought-down-kyc-cost-to-3-from-as-high-as-700-says-nirmala-sitharaman/article66740192.ece > accessed 21 October 2023

[11] David S. Evans, 'Why Can't Europe Create Digital Businesses' (2024) Berkeley Research Group, 37 <https://papers.ssrn.com/sol3/papers.cfm?ab- stract_id=4781503 > accessed 11 July 2024

[12] David Clancy, 'An Update on Twitch in Korea', (Twitch, 5 December 2023) <https://blog.twitch.tv/en/2023/12/05/an-update-on-twitch-in-korea/ > accessed 11 July 2024

[13] Neelanjana Sharma, 'Discussion Paper : Impact of Unnecessary Compliances on Ease of Doing Digital Business in India', (2022) CUTS International, 3-4 <https://cuts-ccier.org/pdf/dp-on-impact-of-unnecessary-compliances-ease-of-doing-digital-business-in-india.pdf> accessed 12 July 2024

[14] Moneycontrol News, 'Indian companies continue to pay high cost of compliance, report says' (Moneycontrol, 8 July 2020) <https://www.moneycon- trol.com/news/business/indian-companies-continue-to-pay-a-high-cost-for-compliance-report-says-5521041.html> accessed 12 July 2024; Times of India, 'India Inc has to deal with 1,536 Acts, 69,233 compliances' (Times of India, 2 May 2024) <https://timesofindia.indiatimes.com/business/india-business/computacenter-inaugurates-new-office-in-bengaluru-koramangala/articleshow/111108052.cms> accessed 12 July 2024.

[15] Neelanjana Sharma, 'Discussion Paper : Impact of Unnecessary Compliances on Ease of Doing Digital Business in India', (2022) CUTS International, 22 <https://cuts-ccier.org/pdf/dp-on-impact-of-unnecessary-compliances-ease-of-doing-digital-business-in-india.pdf> accessed 12 July 2024

[16] Citizens for Justice and Peace 'Why the CAA + NPR + NRC is a toxic cocktail for everyone' (Citizens for Justice, 27 January 2020) <https://cjp.org.in-/why-the-caanprnrc-is-a-toxic-cocktail-for-everyone/#:~:text=At%20least%2042%25%20> accessed 20 February 2024

[17] Citizens for Justice and Peace 'Why the CAA + NPR + NRC is a toxic cocktail for everyone' (Citizens for Justice, 27 January 2020) <https://cjp.org.in/why-the-caanprnrc-is-a-toxic-cocktail-for-everyone/#:~:text=At%20least%2042%25%20> accessed 20 February 2024

Chapter II: Exploring user verification and anonymity

[18] Corey L Guenther, Emily Wilton and Rachel Fernandes, 'Identity' Encyclopaedia of Personality and Individual Differences (Springer, 2020), 2136 <https://link.springer.com/referenceworkentry/10.1007/978-3-319-24612-3_1132#citeas> accessed 10 October 2023

[19] Article 29 Data Protection Working Party, 'Opinion 4/2007 on the concept of personal data' (20 June 2007) <https://ec.europa.eu/justice/article-29/documenta- tion/opinion-recommendation/files/2007/wp136_en.pdf>, accessed 17 July 2024

[20] Office of the Privacy Commissioner of Canada, 'Guidelines for Identification and Authentication' (June 2016) <https://www.priv.gc.ca/en/privacy-topics/identi- ties/identification-and-authentication/auth_061013/> accessed 20 May 2024

[21] The Word Bank Group, 'Identity Authentication and Verification fees: Overview Of Current Practices' (April 2019), 1 <https://documents1.worldbank.org/curat- ed/en/945201555946417898/pdf/Identity-Authentication-and-Verification-Fees-Overview-of-Current-Practices.pdf> accessed 23 May 2024

[22] The Aadhaar (Authentication and Offline Verification) Regulations 2021

[23] Helen Nissenbaum, 'The Meaning of Anonymity in an Information Age' (1999) 15 The Information Society 141 <https://nissenbaum.tech.cornell.edu/pa- pers/The%20Meaning%20of%20Anonymity%20in%20an%20Information%20Age.pdf>

[24] Sudhanshu Chauhan and Nutan Kumar Panda, Hacking Web Intelligence Open-Source Intelligence and Web Reconnaissance Concepts and Techniques (Syngress, 2015)

[25] Jeffrey M Skopek, 'Reasonable Expectations of Anonymity' (2016) 101 Virginia Law Review 691 <https://papers.ssrn.com/sol3/papers.cfm?ab- stract_id=2523393#> accessed 16 October 2023.

[26] UNGA 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye' 29th Session A/HRC/29/3 (2015)

[27] Rahul Matthan, 'End-to-end encryption must be retained at all cost' (Live Mint, 27 August 2019) <https://www.livemint.com/opinion/online-views/opin- ion-end-to-end-encryption-must-be-retained-at-all-cost-1566926664869.html> accessed 20 October 2023

[28] International Communication Association, 'To reveal or not to reveal: A theoretical model of anonymous communication' (1998) 8(4) Communication Theory, 381-407

[29] International Communication Association, 'To reveal or not to reveal: A theoretical model of anonymous communication' (1998) 8(4) Communication Theory, 381-407

[30] Lina Eklund, Emma von Essen, Fatima Jonsson and Magnus Johansson, 'Beyond a Dichotomous Understanding of Online Anonymity: Bridging the Macro and Micro Level' (2021) 27(2) Sociological Research Online 481 <https://journals.sagepub.cdoi/10.1177/13607804211019760#:~:text=Studying%20our%20two%20cases%20has,three%20main%20forms%3B%20by%20factual> accessed 16 October 2023

[31] Helen Nissenbaum, 'The Meaning of Anonymity in an Information Age' (1999) 15 The Information Society 141 <https://nissenbaum.tech.cornell.edu/pa- pers/The%20Meaning%20of%20Anonymity%20in%20an%20Information%20Age.pdf>

[32] A. Michael Froomkin, 'Lessons Learned Too Well: Anonymity in a Time of Surveillance' (2017) 59 Arizona Law Review 95 <https://repository.law.miami.edu/c- gi/viewcontent.cgi?article=1311&context=fac_articles

[33] Demos, 'Why online anonymity is vital in a healthy democratic society' (Demos, 10 January 2022) <https://demos.co.uk/blogs/why-online-anonymity-is-vi- tal-in-a-healthy-democratic-society/> accessed 16 October 2023.

[34] UNGA, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye' (22 May 2015) 29th Session A/HRC/29/3, 4.

[35] KS Puttaswamy v Union of India (2017) 10 SCC 1, Part L, para 141; See also CPIO v Subhash Chandra Agarwal (CPIO judgment), the Supreme Court observed that the right to anonymity falls within the scope of the right to privacy.

[36] Rishab Bailey, Vrinda Bhandari, and Faiza Rahman, 'Examining the Online Anonymity Debate: How far should the law go in mandating user identification?' (2021) Working Paper 18, Data Governance Network 1, 8 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4023323> accessed 10 October 2023

[37] Jeffrey M Skopek, 'Reasonable Expectations of Anonymity', (2016) 101 Virginia Law Review <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2523393#> accessed 16 October 2023

[38] Roshan H Nair, 'Indian Twitter Is a Bastion of Masked Troll-Slayers', (Deccan Herald, 04 August 2019) <https://www.deccanherald.com/india/karnataka/bengal- uru/indian-twitter-is-a-bastion-of-masked-troll-slayers-751967.html> accessed 16 October 2023

[39] Yashraj Sharma and Gafira Qadir, 'People Are Vanishing: In Kashmir, Twitter Users Remove Digital Footprints as Police Cracks Whip', (The Kashmir Walla, 14 August 2020) <https://thekashmirwalla.com/people-are-vanishing-in-kashmir-twitter-users-remove-digital-footprints-as-police-cracks-whip/> accessed 16 October 2023

[40] Yaman Akdeniz, 'Anonymity, Democracy, and Cyberspace' (2002) 69(1) Social Research 180 <https://www.researchgate.net/publication/292865703_Anonymi-ty_democracy_and_cyberspace> accessed 16 October 2023

[41] Catherine Thorbecke, 'How tech has fueled a 'leaderless protest' in Hong Kong' (ABC News, 2 October 2019) <https://abcnews.go.com/Technology/tech-fueled- leaderless-protest-hong-kong/story?id=66158665> accessed 7 January 2024 ; Springer, 'Being Hidden and Anonymous' in 'Cyber Security: Issues and Current Trends' (October 2021)

[42] Catherine Thorbecke, 'How tech has fueled a 'leaderless protest' in Hong Kong' (ABC News, 2 October 2019) <https://abcnews.go.com/Technology/tech-fu-eled- leaderless-protest-hong-kong/story?id=66158665> accessed 7 January 2024 ; Springer, 'Being Hidden and Anonymous' in 'Cyber Security: Issues and Current Trends' (October 2021)

[43] Rishab Bailey, Vrinda Bhandari, and Faiza Rahman, 'Examining the Online Anonymity Debate: How far should the law go in mandating user identification?' (2021) Working Paper 18, Data Governance Network 1, 8 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4023323> accessed 10 October 2023

[44] Jeffrey M Skopek, 'Reasonable Expectations of Anonymity', (2016) 101 Virginia Law Review <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2523393#> accessed 16 October 2023

[45] Andrea Burzynski, 'How one Egyptian sold revolution on the Web' (Reuters, 20 January 2012) <https://www.reuters.com/article/idUSDEE80I0MV/> accessed 7 January 2024

[46] Terry Halsch, 'Anonymous Tip Technology Helps Law Enforcement Solve Crime' (Police Chief, 2022) <https://www.policechiefmagazine.org/tip411-anony- mous- tip-technology-helps-law-enforcement-solve-crimes/> accessed 7 January 2024.

[47] Sarah C Nicksa, 'Bystander's Willingness to Report Theft, Physical Assault, and Sexual Assault: The Impact of Gender, Anonymity, and Relationship With the Offender' (2014) 29 Journal of Interpersonal Violence 217, 221.

[48] The National Cyber Crime Reporting Portal allows anonymous reporting of online Child Pornography or sexually explicit content such as Rape/Gang Rape content <https://cybercrime.gov.in/Webform/FAQ.aspx>

[49] Karina Rigby, 'Anonymity on the Internet Must be Protected' (1995) Ethics and Law on the Electronic Frontier <https://groups.csail.mit.edu/mac/classes/6.805/ stu-dent-papers/fall95-papers/rigby-anonymity.html> accessed 7 January 2024

[50] Por Henrick Amstrong and Joy Liddicoat, 'The Rights to Freedom of Peaceful Assembly and Association and the Internet: Submission to the United Nations Special Rapporteur on the Rights to Freedom of Peaceful Assemblyand Association' (January 2012) cited in Association for Progressive Communication, 'The right to freedom of speech and expression and the use of encryption in the digital communications: Submissions to the United Nations Special Rapporteur on the Right to Freedom of Opinion and Expression by the Association or Progressive Communication (February 2015) 1, 4 <https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/AssociationForProgressiveCommunication.pdf> accessed 7 January 2024

[51] Clifford Olanday, 'How this inspirational social activist gives power to survivors of sexual violence' (Tatler, 29 July 2023) <https://www.tatlerasia.com/power-pur- pose/front-female/elsamarie-d-silva-safecity-red-dot-foundation-brave-movement?

[52] Poorva Joshi, 'A platform allows victims of sexual harassment to share their stories anonymously'(Hindustan Times, 25 March 2017) <https://www.hindustan- times.com/more-lifestyle/a-website-allows-victims-of-sexual-harassment-to-share-their-stories-anonymously/story-iZwYuMT2cYDREG8OreiCON.html > accessed 7 January 2024

[53] The Whistleblower Protection Act, 2014

[54] S. 72, Bharatiya Nyaya Sanhita 2023 ; Erstwhile S. 228A, Indian Penal Code

[55] S.23, The Protection of Children from Sexual Offences Act, 2012.

[56] S. 34, HIV and AIDS (Prevention and Control) Act, 2017

[57] Anthony D. Ong and David J Weiss, 'The impact of anonymity on responses to sensitive questions' (1999) 30 Journal of Applied Social Psychology 1691, 1702 <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=6d63fcaf1cf92da204fdb5dc651a2ba62c88dba5> accessed 7 October 2023

[58] Johanna Simfors and Rasmus Rudling, 'How does the degree of anonymity affect our morals? : A study examining behavioural changes in online communication' (2020) Vetenskap Och Konst <https://www.diva-portal.org/smash/get/diva2:1440921/FULLTEXT01.pdf> accessed 7 January 2024

[59] Johanna Simfors and Rasmus Rudling, 'How does the degree of anonymity affect our morals? : A study examining behavioural changes in online communication' (2020) Vetenskap Och Konst <https://www.diva-portal.org/smash/get/diva2:1440921/FULLTEXT01.pdf> accessed 7 January 2024

[60] Danielle Citron, 'Cyber Civil Rights', (2009) 89 Boston University Law Review 61, 64

[61] M. E. Kabay, 'Anonymity and Pseudonymity in Cyberspace: Deindividuation, Incivility and Lawlessness Versus Freedom and Privacy' (Annual Conference of the European Institute for Computer Anti-virus Research (EICAR), Munich, Germany 16 March 1998) <https://www.mekabay.com/overviews/anonpseudo.pdf> accessed 7 January 2024

[62] Tamara Littleton, 'Why Do People Become Trolls Online?' (The Social Element, 21 October 2020) <https://thesocialelement.agency/why-people-become-trolls-on- line> accessed 16 October 2023

[63] John Markoff, 'Internet's Anonymity Makes Cyberattack Hard to Trace', (The New York Times, 16 July 2009) <https://www.nytimes.com/2009/07/17/ technology/17-cyber.html> accessed 17 October 2023

[64] eSafety Commissioner, 'Anonymity and identity shielding' (eSafety Commissioner, 17 February 2024) <https://www.esafety .gov.au/industry/tech-trends-and-chal- lenges/anonymity> accessed 3 March 2024

[65] Goodison, Sean E., Dulani Woods, Jeremy D. Barnum, Adam R. Kemerer, and Brian A. Jackson, 'Identifying Law Enforcement Needs for Conducting Criminal Investigations Involving Evidence on the Dark Web', RAND Corporation (29 October 2019) <https://www.rand.org/pubs/research_reports/RR2704.html>

Chapter III: Evaluating the need for user verification measures on social media platforms

[66] Financial Action Task Force, 'Recommendation 10: Customer Due Diligence' (2012) <https://www.cfatf-gafic.org/documents/- fatf-40r/376-fatf-recommendation-10-customer-due-diligence> accessed 17 October 2023

[67] R. 9(1)(a), (b), Prevention of Money Laundering (Maintenance of Records) 2005

[68] Paragraph 13, RBI Master Direction - Know Your Customer (KYC) Direction, 2016 <https://www.rbi.org.in/CommonPerson/english/scripts/notifica- tion.aspx?id=2607#13> accessed 17 October 2023

[69] Paragraph 3 (a) XIX, RBI Master Direction - Know Your Customer (KYC) Direction, 2016 <https://www.rbi.org.in/CommonPerson/english/scripts/notifica- tion.aspx?id=2607#13> accessed 17 October 2023

[70] Paragraph 16, RBI Master Direction Know Your Customer (KYC) Direction 2016, <https://www.rbi.org.in/CommonPerson/english/scripts/notifica- tion.aspx?id=2607#13> accessed 17 October 2023

[71] Paragraph 8.2, IRDAI Master Guidelines on Anti-Money Laundering/ Counter Financing of Terrorism (AML/CFT), 2022, <https://irdai.gov.in/docu- ments/37343/366029/Mas-ter+Guidelines+on+Anti-Money+Laundering+2022.pdf/0e50dd32-00f3-33e1-ebee-0d0989d67932?version=1.1&t=1665032662486&download=true>accessed 17 October 2023

[72] Paragraph 33, Securities Exchange Board of India Master Circular on Know Your Client (KYC) norms for the securities market <https://www.sebi.gov.in/legal/ mas-ter-circulars/oct-2023/master-circular-on-know-your-client-kyc-norms-for-the-securities-market_77945.html> accessed 17 October 2023

[73] R. 7 (1), Aadhaar (Authentication and Offline Verification) Regulations, 2021

[74] S. 2(c), Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

[75] Unique Identification Authority of India, Secure QR Code Reader <https://uidai.gov.in/en/ecosystem/authentication-devices-documents/qr-code-reader.html> accessed 17 October 2023.

[76] Reserve Bank of India, Master Direction Know Your Customer (KYC) Direction 2016 <https://www.rbi.org.in/CommonPerson/english/scripts/notifica- tion.aspx?id=2607#13> accessed 17 October 2023

[77] Clause 39.17, Unified Access Service License; Sudeshna Mitra, 'Govt Tightens KYC Process For Mobile SIM Cards To Check Cybercrimes' (Inc42, 18 August 2023) <https://inc42.com/buzz/govt-tightens-kyc-process-for-mobile-sim-cards-to-check-cybercrimes/> accessed 20 October 2023.

[78] Rishab Bailey, Vrinda Bhandari, and Faiza Rahman, 'Examining the Online Anonymity Debate: How far should the law go in mandating user identification?' (2021) Working Paper 18, Data Governance Network< https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4023323> accessed 10 October 2023.

[79] Clause 7.1, Unified Access Service License, read with Clause 39.20, Unified Access Service License.

[80] S.3(7), the Telecommunications Act 2023.

[81] Paul Koshy, 'The Alarming Provisions of India's New Telecommunications Act' , (The Wire, 8 January 2024) <https://thewire.in/government/the-alarming-provi- sions-of-indias-new-telecommunications-act> last accessed 23 May 2024

[82] LiveMint, 'CoWIN Data leak! Aadhaar, PAN Card info, share on Covid vaccination portal, made by Telegram: report' (LiveMint, 12 June 2023) <https://www.live- mint.com/news/india/cowin-data-leak-data-bre-ach-aarogya-setu-aadhaar-pan-card-shared-on-covid-vaccination-portal-available-on-telegram-11686549051340.html> accessed 10 October 2023

[83] Hindustan Times, 'Aadhaar details of 81.5 cr people leaked India's 'biggest data breach' (Hindustan Times, 31 October 2023) <https://www.hindustan- times.com/technology/in-indias-biggest-data-breach-personal-information-of-81-5-crore-people-leaked-101698719306335.html> accessed 10 October 2023.

[84] R. 4(2), Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

[85] Rishab Bailey, Vrinda Bhandari, and Faiza Rahman, 'Examining the Online Anonymity Debate: How far should the law go in mandating user identification?' (2021) Data Governance Network, Working Paper 18/2021 1, 24-25 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4023323> accessed 10 October 2023

[86] Aditi Agarwal 'Can traceability and end-to-end encryption co-exist?' (Forbes India, 17 March 2021) <https://www.forbesindia.com/article/take-one-big-story-of-the-day/can-traceability-and-endtoend-encryption-coexist-heres-the-legal-view/67001/1> accessed 11 October 2023

[87] UNGA, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye' (22 May 2015) 29th Session A/HRC/29/3

[88] WhatsApp LLC v Union of India W.P. (C) 7284/2021

[89] Aditi Agarwal 'Can traceability and end-to-end encryption co-exist?' (Forbes India, 17 March 2021) <https://www.forbesindia.com/article/take-one-big-sto- ry-of-the-day/can-traceability-and-endtoend-encryption-coexist-heres-the-legal-view/67001/1> accessed 11 October 2023

[90] Software Freedom Law Centre, 'Right to Encrypt: Subset of Right to Privacy?' (Software Freedom Law Centre, 2021), <https://sflc.in/right-encrypt-sub-set-right-privacy/> accessed on 12 October 2023

[91] Sofi Ahsan, 'Tracing messages will violate privacy, chill free speech: WhatsApp', (The Indian Express, 27 May 2021) < https://indianexpress.com/article/technolo-gy/tech-news-technology/tracing-messages-will-violate-privacy-chill-free-speech-whatsapp-7331846/>

[92] KS Puttaswamy v Union of India (2017) 10 SCC 1, Part S, para 180

[93] Ministry of Electronics and Information Technology, Right to Privacy is a Fundamental Right (2021) <https://www.pib.gov.in/PressReleseDetailm.aspx-?PRID=1721915> accessed 13 October 2023

[94] Ministry of Electronics and Information Technology, Right to Privacy is a Fundamental Right (2021) <https://www.pib.gov.in/PressReleseDetailm.aspx-

[95] Greg Nojeim and Namrata Maheshwari, 'Encryption in India: preserving the Online Engine of Privacy, Expression, Security, and Economic Growth' (2021) 17 Indian Journal of Law and Technology 1, 16

[96] Vasudev Devadasan, 'Report on Intermediary Liability in India' (2022) Centre for Communication Governance 1, 81 <https://ccgdelhi.s3.ap-south-1.ama- zonaws.com/uploads/reportonintermediaryliabilityinindia-web-180123-344.pdf> accessed 10 October 2023

[97] Antony Clement v Union of India, W.P. No. 20774/2018; In this case, Dr. V. Kamakoti, Director, Indian Institute of Technology, Madras, submitted an affidavit suggesting that the first originator of the message can be traced by attaching the information of the originator to the message

[98] Greg Nojeim and Namrata Maheshwari, 'Encryption in India: preserving the Online Engine of Privacy, Expression, Security, and Economic Growth' (2021) 17 Indian Journal of Law and Technology 1, 16

[99] Vasudev Devadasan, 'Report on Intermediary Liability in India' (2022) Centre for Communication Governance 1, 87.

[100] Vasudev Devadasan, 'Report on Intermediary Liability in India' (2022) Centre for Communication Governance 1, 79.

[101] Rule 4(2), IT Rules; The provision requires an intermediary to only identify first originator of information on their computer resource upon receiving a judicial order or an order passed by the Competent Authority under Section 69 of the IT Decryption Rules.

[102] Vasudev Devadasan, 'Report on Intermediary Liability in India' (2022) Centre for Communication Governance 1, 79.

[103] Gushabad Grover, Tanya Rajwade and Divyank Kataria, 'The Ministry and the Trace: Subverting End-to-End Encryption' (2021) 14 NUJS Law Review 224, 231; In this paper, the authors presume the 'first originator' to be the person who introduces the message on the platform, therefore, the "absolute originator". They further define relative originators as people who sent the same message independently which leads to multiple chains of forwarded messages.

[104] Aishani Rai and Sarayu Natrajan, 'Unpacking Social and Economic Gains from Encryption', Aapti Institute (November 2021) 1,10 <https://broadbandindiafo- rum.in/wp-content/uploads/2021/12/Aapti_BIF_Encryption-Report.pdf > accessed 30 January 2024.

[105] Ministry of Electronics and Information Technology, Right to Privacy is a Fundamental Right (2021) <https://www.pib.gov.in/PressReleseDetailm.aspx-?PRID=1721915> accessed 13 October 2023.

[106] WhatsApp LLC v Union of India, WP (Crl.) No. 02 of 2023, order dated 26 September 2023 <https://drive.google.com/file/d/1d90QOvTP8J2Lc- MaCh-SJo8qn7sLZi1K5/view?usp=sharing> accessed 17 October 2023.

[107] Farkhanda Zahoor, 'How A Bill Becomes A Zombie? The Journey of Section 66A of the Information Technology Act, 2000' (Internet Freedom Foundation, 18 May 2020) <https://internetfreedom.in/how-a-bill-becomes-a-zombie-the-journey-of-section-66a-of-the-information-technology-act-2000/>, accessed on 29 January 2024.

[108] Abhinav Sekhri and Apar Gupta, 'Section 66A and Other Legal Zombies' (31 October 2018) IFF Working Paper No. 2/2018, 2 <http://dx.doi.org/10.2139/ss- rn.3275893> accessed 17 October 2023.

[109] Art. 30, Enforcement Decree on Information and Communications Network Act, Presidential Decree No. 20668

[110] Art. 30, Enforcement Decree on Information and Communications Network Act, Presidential Decree No. 21278 'South Korea's Real-Name Net Law Is Rejected by Court' (BBC News, 23 August 2012) <https://www.bbc.com/news/technology-19357160> accessed 21 October 2023.

[111] 'South Korea's Real-Name Net Law Is Rejected by Court' (BBC News, 23 August 2012) <https://www.bbc.com/news/technology-19357160> accessed 21 October 2023.

[112] David Caragliano, 'Real Names and Responsible Speech: The Cases of South Korea, China, and Facebook' (Yale Journal of International Affairs, 21 May 2013) <https://www.yalejournal.org/publications/real-names-and-responsible-speech-the-cases-of-south-korea-china-and-facebook> accessed 21 October 2023.

[113] 24-2(A) KCCR 590, 2010Hun Ma47, 252 (consolidated), August 23, 2012

[114] Electronic Frontier Foundation, 'Mandatory Data Retention' (Electronic Frontier Foundation, 2023) <https://www.eff.org/issues/mandatory-data- retention#:~:text=-Mandatory%20data%20retention%20regimes%20are,%2C%20anonymity%2C%20and%20free%20expression> accessed 20 October 2023.

[115] Catherine Crump, 'Data Retention: Privacy, Anonymity, and Accountability Online' (2003) 56 Stanford Law Review 191.

[116] CERT-In Directions para (v)

[117] Springer, 'Being Hidden and Anonymous' in 'Cyber Security: Issues and Current Trends' (October 2021)

[118] T. Braun, M. Günter, M. Kasumi, I. Khalil, 'Virtual Private Network Architecture' (April 1999)

[119] Varsha Bansal, 'VPN Providers Flee India as a New Data Law Takes Hold' (Wired, 25 September 2022) <https://www.wired.co.uk/article/vpn-firms-flee-india- da-ta-collection-law> accessed 12 October 2023

[120] Varsha Bansal, 'VPN Providers Flee India as a New Data Law Takes Hold' (Wired, 25 September 2022) <https://www.wired.co.uk/article/vpn-firms-flee-india- da-ta-collection-law> accessed 12 October 2023

[121] Suraksha P, 'Delhi HC seeks Cert-In's response to plea challenging cybersecurity directions' (Economic Times, 28 September 2022) <https://economictimes.indi- atimes.com/tech/technology/delhi-hc-seeks-cert-ins-response-to-plea-challenging-cybersecurity-directions/articleshow/94515396.cms?from=mdr>, accessed 17 July 2024

[122] See Counter affidavit filed by CERT-In in the case of SNT Hostings v Union of India <https://drive.google.com/file/d/1Cr_86dhx_WYqVm9RE18btX-ni44CZlfB4/ view?usp=sharing> accessed 16 October 2023.

[123] Digital Personal Data Protection Act, 2023.

[124] S. 2(i), DPDP Act, 2023.

[125] Clifford Olanday, 'How this inspirational social activist gives power to survivors of sexual violence' (Tatler, 29 July 2023) <https://www.tatlerasia.com/power-pur- pose/front-female/elsamarie-d-silva-safecity-red-dot-foundation-brave-movement?

[126] Sourabh Lele, 'DPDP Act: Social media, telecos, startups lobby for 18-24 months to comply' (Business Standard, 1 October 2023) <https://www.business-stan- dard.com/industry/news/social-media-telcos-lobby-for-18-24-months-to-comply-with-dpdp-act-123100100635_1.html> accessed 13 October 2023.

[127] Suraksha P, 'Verifying ID for social media use could pose security risk: Experts' (Economic Times, 10 August 2023) <https://economictimes.india-times.com/tech/technology/verifying-id-for-social-media-use-could-pose-security-risk-experts/articleshow/102583346.cms?from=mdr > accessed on 10 October 2023.

[128] Suraksha P, 'Verifying ID for social media use could pose security risk: Experts' (Economic Times, 10 August 2023) <https://economictimes.india- times.com/tech/technology/verifying-id-for-social-media-use-could-pose-security-risk-experts/articleshow/102583346.cms?from=mdr > accessed on 10 October 2023.

[129] Suraksha P, 'Verifying ID for social media use could pose security risk: Experts' (Economic Times, 10 August 2023) <https://economictimes.india- times.com/tech/technology/verifying-id-for-social-media-use-could-pose-security-risk-experts/articleshow/102583346.cms?from=mdr > accessed on 10 October 2023.

[130] Suraksha P, 'Verifying ID for social media use could pose security risk: Experts' (Economic Times, 10 August 2023) <https://economictimes.india- times.com/tech/technology/verifying-id-for-social-media-use-could-pose-security-risk-experts/articleshow/102583346.cms?from=mdr > accessed on 10 October 2023.

[131] Gulveen Aulakh and Shouvik Das, 'Data Privacy Rules to Be Issued for Consultation Shortly: Rajeev Chandrasekhar' (Live Mint, 28 December 2023) <https:// w-ww.livemint.com/news/data-privacy-rules-to-be-issued-for-consultation-shortly-rajeev-chandrasekhar-11703772692563.html> accessed 12 February 2024.

[132] Article 19, 'Policy Brief: The Global Principles on Protection of Freedom of Expression and Privacy' (2017) 14, 30 <https://www.article19.org/data/files/mediali- brary/38657/Expression-and-Privacy-Principles-1.pdf> accessed 10 October 2023.

[133] Central Public Information Officer, Supreme Court of India v Subhash Chandra Agarwal, (2020) 5 SCC 481, para 44-47. See also KS Puttaswamy v Union of India (2017) 10 SCC 1, Part S, para 180.

[134] Anuradha Bhasin v Union of India, 2020 (3) SCC 637, para 67-70.

[135] Greg Nojeim and Namrata Maheshwari, 'Encryption in India: Preserving the Online Engine of Privacy , Expression, Security, and Economic Growth' (2021) 17 Indian Journal of Law and Technology 1, 29.

[136] Vasudev Devadasan, 'Report on Intermediary Liability in India' (2022) Centre for Communication Governance 1, 88.

[137] Electronic Frontier Foundation, 'Surveillance and Self Defense: Metadata' <https://ssd.eff.org/glossary/metadata> accessed 20 October 2023.

[138] Vasudev Devadasan, 'Report on Intermediary Liability in India'(2022) Centre for Communication Governance 1, 81 <https://ccgdelhi.s3.ap-south-1.ama- zonaws.com/uploads/reportonintermediaryliabilityinindia-web-180123-344.pdf> accessed 10 October 2023.

[139] Gurshabad Grover, Tanaya Rajwade & Divyank Katira, 'The Ministry and the Trace: Subverting End-To-End Encryption' (2021) 14 NUJS Law Review 224, 234 <http://nujslawreview.org/wp-content/uploads/2021/07/14.2-Grover-Rajwade-Katira-2.pdf> accessed 16 October 2023.

[140] Gurshabad Grover, Tanaya Rajwade & Divyank Katira, 'The Ministry and the Trace: Subverting End-To-End Encryption' (2021) 14 NUJS Law Review 224, 234 <http://nujslawreview.org/wp-content/uploads/2021/07/14.2-Grover-Rajwade-Katira-2.pdf> accessed 16 October 2023.

[141] Rishab Bailey, Vrinda Bhandari, and Faiza Rahman, 'Examining the Online Anonymity Debate: How far should the law go in mandating user identification?' (2021) Data Governance Network, Working Paper 18 29-30 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4023323> accessed 16 October 2023.

[142] Mohammad Meraj Mirza and Umit Karabiyik, 'Enhancing IP Address Geocoding, Geolocating and Visualization for Digital Forensics' (2021) International Symposium on Networks, Computers and Communications, 1.

[143] Mohammad Meraj Mirza and Umit Karabiyik, 'Enhancing IP Address Geocoding, Geolocating and Visualization for Digital Forensics' (2021) International Symposium on Networks, Computers and Communications, 1.

[144] Vikas Mishra, Pierre Laperdrix, Antoine Vastel, Walter Rudametkin, Romain Rouvoy, and Martin Lopatka, 'Don't Count Me Out: On the Relevance of IP Address in the Tracking Ecosystem' (WWW'20: Proceedings of The Web Conference, Tapeï, 28 January 2020) <https://research.mozilla.org/files/2020/02/mishra-www20.pd- f> accessed 16 October 2023.

[145] Gitesh Shelke and Mihir Tanksale, 'Maharashtra: IP address of internet calls stump online fraud sleuths' (Times of India, 28 April 2023) <https:// timesofindia.indi-atimes.com/city/pune/maharashtra-ip-address-of-internet-calls-stump-online-fraud-sleuths/articleshow/99828275.cms> accessed 29 January 2024.

[146] Rishab Bailey, Vrinda Bhandari, and Faiza Rahman, 'Examining the Online Anonymity Debate: How far should the law go in mandating user identification?' (2021) Data Governance Network, Working Paper 18 29-30 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4023323> accessed 16 October 2023.

[147] Mark Stanislav, Two-factor authentication (IT Governance Publishing, 2015).

[148] Alexander Mühle, Andreas Grüner, Tatiana Gayvoronskaya, Christoph Meinel, 'A survey on essential components of a self-sovereign identity' (2018) 30 Computer Science Review <https://www.sciencedirect.com/science/article/abs/pii/S1574013718301217> accessed 16 October 2023.

[149] Uwe Der, Stefan Jähnichen, and Jan Sürmeli, 'Self-sovereign identity opportunities and challenges for the digital revolution' (2017) <https://arx- iv.org/abs/1712.01767> accessed 16 October 2023.

[150] Uwe Der, Stefan Jähnichen, and Jan Sürmeli, 'Self-sovereign identity opportunities and challenges for the digital revolution' (2017) <https://arx- iv.org/abs/1712.01767> accessed 16 October 2023.

[151] Public Official Election Act 2005, art 82(6).

[152] Article 44 (5), The Act on Promotion of Information and Communications Network Utilization and Data Protection 2008

[153] BBC News, 'South Korea's Real-Name Net Law Is Rejected by Court' (BBC News, 23 August 2012) <https://www.bbc.com/news/technology-19357160> accessed 21 October 2023.

[154] Electronic Frontier Foundation, 'Comments submitted to the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (10 February 2015) <https://www.eff.org/node/58485> accessed 21 October 2023.

[155] David Caragliano, 'Real Names and Responsible Speech: The Cases of South Korea, China, and Facebook' (Yale Journal of International Affairs, 21 May 2013) <https://www.yalejournal.org/publications/real-names-and-responsible-speech-the-cases-of-south-korea-china-and-facebook> accessed 21 October 2023.

[156] 2010 Hun-Ma47, KCCR: 24-2(A) KCCR 590.

[157] David Caragliano, 'Real Names and Responsible Speech: The Cases of South Korea, China, and Facebook' (Yale Journal of International Affairs, 21 May 2013) <https://www.yalejournal.org/publications/real-names-and-responsible-speech-the-cases-of-south-korea-china-and-facebook> accessed 21 October 2023; 2010 Hun-Ma47, KCCR: 24-2(A) KCCR 590.

[158] 2020Hun-ma406 (consolidated), 28 January, 2021

[159] 2020Hun-ma406 (consolidated), 28 January, 2021

[160] Law No. 12.965, 23 April 2014.

[161] Rishab Bailey, Vrinda Bhandari and Faiza Rahman, 'Examining the Online Anonymity Debate: How Far Should the Law Go in Mandating User Identification?' (2021) Data Governance Network Working Paper 18
<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4023323> accessed 21 October 2023.

[162] Isaura Silva, Douglas Leite and Fernanda Cohen, 'Sarahah and Secret: Notes on Apparent Anonymity in Internet Applications' (Migalhas, 8 August 2017) <https://www.migalhas.com.br/depeso/263414/sarahah-e-secret--notas-sobre-o-anonimato-aparente-em-aplicativos-de-internet> accessed 20 October 2023.

[163] Freedom House, 'Brazil: Freedom on the Net 2021 Country Report' (Freedom House)
<https://freedomhouse.org/country/brazil/freedom-net/2021> accessed 21 October 2023.

[164] Tales Tomaz, 'Brazilian Fake News Bill: Strong Content Moderation Accountability but Limited Hold on Platform Market Power' (2023) 30 Journal of the European Institute for Communication and Culture 253 <https://www.tandfonline.com/doi/full/10.1080/13183222.2023.2201801> accessed 20 October 2023; Veridiana Alimonti, 'Brazil's Fake News Bill: Congress Must Stand Firm on Repealing Dangerous and Disproportionate Surveillance Measures' (Electronic Frontier Founda-tion, 10 November 2021) <https://www.eff.org/deeplinks/2021/11/brazils-fake-news-bill-congress-must-stand-firm-repealing-dangerous-and> accessed 20 October 2023.

[165] Human Rights Watch, 'Brazil: Reject "Fake News" Bill' (Human Rights Watch, 28 October 2020)
<https://www.hrw.org/news/2020/06/24/brazil-reject-fake-news-bill> accessed 20 October 2023.

[166] Brazilian Law on Freedom, Responsibility and Transparency on the Internet (Bill) 2020.

[167] 'Katitza Rodriguez and Seth Schoen', '5 Serious Flaws in the New Brazilian "Fake News" Bill that Will Undermine Human Rights [UPDATED]' (Electronic Frontier Foundation, 29 June 2020)
<https://www.eff.org/deeplinks/2020/06/5-serious-flaws-new-brazilian-fake-news-bill-will-undermine-human-rights> ; Veridiana Alimonti, 'Brazil's Fake News Bill: Congress Must Stand Firm on Repealing Dangerous and Disproportionate Surveillance Measures' (Electronic Frontier Foundation, 10 November 2021)
<https://www.eff.org/deeplinks/2021/11/brazils-fake-news-bill-congress-must-stand-firm-repealing-dangerous-and> accessed 20 October 2023.

[168] Online Safety Act 2023.

[169] S. 81(2), Online Safety Act 2023,

[170] S. 230(2), Online Safety Act 2023,

[171] S. 230(3), Online Safety Act 2023,

[172] 'Online Safety Bill: US and UK Campaigners Warn of Dangers of Age Verification' (Open Rights Group, 5 September 2023) <https://www.openrightsgroup.org/press-releases/online-safety-bill-us-and-uk-campaigners-warn-of-dangers-of-age-verification/> accessed 20 October 2023

[173] Ofcom, 'draft Guidance on age assurance and other Part 5 duties for service providers for publishing pornographic content on online services' (5 December 2023) <https://www.ofcom.org.uk/ data/assets/pdf_file/0018/272601/guidance-part-5-annexe-2.pdf > accessed 30 January 2024

[174] UK Government and Parliament Petitions, 'Petition: Make Verified ID a Requirement for Opening a Social Media Account' (2021) <https://petition.parliament.uk/petitions/575833> accessed 6 October 2023

[175] European Commission, 'Press Corner Questions and answers on the impact of the Digital Services Act' (European Commission, 23 February 2024) <https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348> accessed 16 May 2024.

[176] Case C-623/17 Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others EU:C: 2020:790, paragraph 57.

[177] Oliver Noyan, 'German Supreme Court Orders Facebook to Allow Pseudonyms' (www.euractiv.com, 28 January 2022) <https://www.euractiv.com/section/data-protection/news/german-supreme-court-orders-facebook-to-allow-pseudonyms/> accessed 21 October 2023.

[178] S. 13(6),Telemedia Act 2007,

[179] Florian Richter, 'Online Regulation: Germany's Plans to Tackle "Digital Violence" (and Likely Other Issues, Too)' (Lexology, 15 May 2023) <https://www.lexology.com/library/detail.asp ?g=67cc1c39-dc71-4a05-9843-54207bc331c2#:~:text=The%20ambi- tiously%20titled%20%E2%80%9-CAct%20against,facilitate%20their%20enforcement%20in%20Germany.> accessed 21 October 2023.

[180] Alina Clasen, 'Germany Plans Legislation to Block Cyber-Hate Accounts' (www.euractiv.com, 13 April 2023) <https://www.euractiv.com/section/platforms/ news/-germany-plans-legislation-to-block-cyber-hate-accounts/> accessed 21 October 2023.

[181] Hannah Fang, 'France Senate Passes Legislation Requiring Age Verification for Minors on Social Media' (Jurist, 30 June 2023) <https://www.jurist.org/news/2023/06/france-senate-passes-legislation-requiring-age-verification-for-minors-on-social-media/> accessed 21 October 2023.

[182] Art 6-7-I, Law no. 2004-575 of 2004

[183] Nicolae Bochis, 'France Pushes for Age Verification for Social Media Platforms' (CyberGhost Privacy Hub, 16 March 2023) <https://www.cyberghostvpn.com/en_US/privacyhub/france-age-verification/> accessed 21 October 2023.

[184] Rosheen Javed, 'France to Implement Age Verification for Social Media Platforms' (Technology Times, 17 March 2023) <https://www.technologytimes.pk/2023/03/17/france-to-implement-age-verification-for-social-media-platforms/> accessed 21 October 2023.

Chapter V: Conclusion and Recommendations

[185] Moneycontrol, 'Internet Users in India Set to Reach 900 Million by 2025: Report' (Moneycontrol, 3 May 2023)<https://www.moneycontrol.com/news/business/internet-users-in-india-set-to-reach-900-million-by-2025-report-10522311.html#google_vignette> accessed 17 October 2023

[186] Centre for Media Transition, 'The future of co-regulation in the digital platform era' (University of Technology Sydney, 14 February 2024)<https://www.uts.edu.au/research/centre-media-transition/projects-and-research/future-co-regulation-digital-platform-era#:~: text=Aiming%20to%20address%20the%20escalating,these%20issues%20on%20digital%20platforms>, accessed 20 May, 2024

[187] The HinduBusinessLine, '66 Million Children Aged 5-11 Years Are Active Internet Users in India' (Hindu BusinessLine, 6 December 2021)<https://www.thehindubusinessline.com/info-tech/66-mn-internet-users-in-india-aged-between-5-and-11-years/article29518418.ece> accessed 18 October 2023