Data Governance Network
Anchored by IDFC Institute

July 2021

Working Paper 18

Examining the Online Anonymity Debate: How far should the law go in mandating user identification?

Rishab Bailey, Vrinda Bhandari and Faiza Rahman

IDFC Institute

Data Governance Network

The Data Governance Network is developing a multi-disciplinary community of researchers tackling India's next policy frontiers: data-enabled policymaking and the digital economy. At DGN, we work to cultivate and communicate research stemming from diverse viewpoints on market regulation, information privacy and digital rights. Our hope is to generate balanced and networked perspectives on data governance — thereby helping governments make smart policy choices which advance the empowerment and protection of individuals in today's data-rich environment.

About Us

The National Institute of Public Finance and Policy (NIPFP) is a centre for research in public economics and policies. Founded in 1976, the institute undertakes research, policy advocacy and capacity building in a number of areas, including technology policy. Our work in this space has involved providing research and policy support to government agencies and contributing to the creation and dissemination of public knowledge in this field. Our current topics of interest include privacy and surveillance reform; digital identity; Internet governance and rights, and regulation of emerging technologies. We also focus on research that lies at the intersection of technology policy, regulatory governance and competition policy.

Disclaimer and Terms of Use

The views and opinions expressed in this paper are those of the authors and do not necessarily represent those of the organisation.

Design

Cactus Communications

Suggested Citation:

Bailey, R., Bhandari, V. & Rahman, F., (2021). *Examining the Online Anonymity Debate: How far should the law go in mandating user identification?* online Data Governance Network Working Paper 18

Supported by a grant from Omidyar Network

Abstract

This paper explore the contours of the right to anonymity in Indian law, and its applicability to the online context. We analyse the arguments made for and against anonymity in the offline context, and demonstrate that typically, careful balancing of competing interests is required before a decision to lift the veil of anonymity. Accordingly, we argue that there should be no general prohibition on online anonymity, whether on social media or otherwise. We then analyse the recent Intermediaries Rules, 2021 that require significant social media intermediaries to (a) enable voluntary verification of users, and (b) trace the originator of information on their platforms if they provide a messaging service. We argue that voluntary verification must remain so. A de facto mandatory requirement for real-name identification, particularly through Aadhaar, could be unconstitutional. Further, a traceability requirement could have disproportionate impacts on rights to privacy and speech. The absence of adequate safeguards in the Intermediaries Rules and the presence of alternative options to trace users also render such an obligation unnecessary and disproportionate. The mere fact that law enforcement cannot always readily access the significant quantities of user data collected in the digital ecosystem cannot be a sufficient ground to bring about systemic change, which could have the cost of further moving India towards a digital surveillance state.

Table of Contents

1. Introduction

The debate between liberty and security and which value should get primacy in modern democracies has been a perennial one, and is equally contested in the space of digital rights. Growing instances of online harm have led to increased demands for the State as well as intermediaries to take steps to make the online ecosystem safer (Bahl, Rahman & Bailey, 2020). The issue of how to identify perpetrators of online offences is therefore a key question facing policymakers today. This is seen as essential in adequately apportioning responsibility and affixing liability.

Despite anonymity not being a design feature of the Internet itself, the difficulty in establishing real-world identities of online users is considered one of the primary factors driving the increase in online offences (Koops, 2010). On the other hand, the degree of anonymity afforded by the Internet is also important in enabling the spread of dissenting ideas, enabling vulnerable individuals and communities to organise, and generally democratising discourse. Given the absence of adequate checks and balances on the State's surveillance and related powers (Bailey, Bhandari, Parsheera & Rahman, 2018), as well as the growing concerns around persecution of dissident and critical voices in India, the relative anonymity offered by the Internet can be vital to protect democratic discourse.

Accordingly, the anonymity versus law enforcement debate is increasingly becoming a public policy concern in India. The absence of clarity on the duties of intermediaries in this regard, and the inability expressed by LEAs to take prompt action pertaining to illegal content has only increased calls for amendments to existing laws. Notably, the draft Personal Data Protection Bill, 2019 ("PDP Bill"), includes a provision requiring the (voluntary) verification of user identity by intermediaries. A similar provision is contained in the recently notified Information Technology (Intermediaries Guidelines) Rules of 2021 ("Intermediary Liability Rules"). Crucially, the Intermediary Liability Rules impose a mandatory traceability requirement on "significant social media intermediaries providing services primarily in the nature of messaging". Such intermediaries are required to enable identification of the "first originator of the information on its computer resource" in India.[1]

WhatsApp has challenged this provision before the High Court of Delhi alleging a breach of privacy rights of its users (Thapliyal, 2021). Previously, various cases had also been filed before courts requiring social media intermediaries in particular, to mandate the linking of real-world identification with social media handles (Web Desk, 2019; Agrawal & Pahwa, 2019).[2]

[1] The platform must have over 50 lakh registered users to qualify as a significant social media intermediary. Rule 4(2) of the IT Rules also limit the use of the 'traceability' power to the detection/prevention/investigation of offences concerning the sovereignty or integrity of India, security of the state, friendly relations with foreign states, public order, incitement of the above cases, or offences relating to distribution of sexually explicit material that are punishable with imprisonment for more than 5 years. An order mandating traceability can only be passed where there are no other less intrusive means available to trace the originator of the information, and further such an order cannot order disclosure of the contents of the message itself.

[2] In 2018, PILs were filed before the Madras High Court seeking the mandatory linking of social media user and email accounts with Aadhaar or any other Government identity proofs. The Court declined to permit this and instead expanded the scope of the petitions to include issues of fake news spreading on social media and traceability of originators of messages on WhatsApp (Agrawal & Pahwa, 2019).

However, the Madras High Court refused to permit the linking of Aadhaar with social media accounts, and the government has stated that Aadhaar linking will not be required for social media accounts.[3]

The debate between anonymity and security interests often brings with it two assumptions: first, that this is a matter of individual rights (of privacy) pitted against public interests (in preventing online crime). However, as we discuss in the paper, anonymity can and does have significant implications and benefits for the public and society at large. Second, that online users are indeed anonymous or that online anonymity is easy to achieve. This ignores the fact that it is often difficult if not impossible for a lay-user to be completely anonymous from all actors in the digital ecosystem (particularly when it comes to large, commercial platforms such as Facebook, WhatsApp, Gmail and the like).[4] Online anonymity in common parlance usually just implies that a user's identity may not be readily apparent to other users or to the State. However intermediaries, ranging from browsers to platforms, do collect significant quantities of personal data in the normal course, which can often be sufficient to identify users. Collection of user data is after all the sine qua non of the business models used by a majority of online platforms.

In this context, this paper attempts to examine the growing debate around online anonymity in India. We first examine what the terms 'anonymity' and 'identification' mean. Then, drawing on legal precedent and literature pertaining to the recognition of anonymity in the offline context, we seek to examine the arguments made for and against online identification mandates. Based on an analysis of these arguments, the paper argues that there should be no general prohibition on online anonymity. We then analyse the voluntary verification and traceability requirements imposed by the recent Intermediary Liability Rules. First, we point to how the voluntary nature of verification must not de facto turn into a real-name identification/verification mandate. Second, we argue that traceability requirements must not seek to introduce systemic weaknesses in the digital ecosystem. The reasons for this include that such a mandate applies to all users irrespective of any evidence of illegal acts, in the process exposing them to privacy harms, and also, because LEAs have sufficient alternative options at hand to identify perpetrators of online offences. The absence of application of a judicial mind to such cases also vitiates the law. Hence, such a mandate may not pass the necessity and proportionality tests as laid down in the Puttaswamy cases, as it would impose significant costs on civil liberties considered essential in a democracy.

The paper is structured as follows: This section introduces the issue. Section 2 first provides a brief overview of the terms "identification" and "anonymity", and then examines the arguments advanced in favour of and against online anonymity, with a view to understand the contours of the "right". Is there a right to anonymity? In what circumstances is this protected and when can it be done away with? In Section 3 we analyse the voluntary verification requirement and examine the constitutionality of the traceability obligation in the recent Intermediary Liability Rules. In Section 4 we briefly outline how the current legal system as well as business models of major online platforms already enable users to be identified, and accordingly argue that measures other than a mandate for traceability or removing anonymity should be adopted to secure the online ecosystem from illegal activities. Section 5 concludes.

[3] The government has informed Parliament that there is no proposal to enact a law for linking Aadhaar with social media accounts of individuals. See response of Minister of Electronics and Information at https://uidai.gov.in //images/loksabha/LSPQ_471_Unstarred.pdf.

[4] The degree of anonymity afforded by social media platforms is largely due to (a) the aggregation effect, and (b) the ability to use pseudonyms, and not because users are truly anonymous from all entities in the ecosystem.

2. Understanding identification and anonymity

In this section, we seek to understand what the terms "identification" and "anonymity" mean, and examine the scope of the right to online anonymity under Indian law.

2.1 Understanding 'identification' and 'anonymity'

The term "identity" is generally understood as referring to the biological/physical, mental, or economic, cultural or social characteristics of a person that differentiate that particular individual from others (Anonymous, 2020b).[5] Identification can therefore be understood as a means to "single out" or distinguish an individual from a group. The amount of information required to "identify" an individual can vary, based on the size of the group at hand and the information in question. For instance, a first name in a large data set may not be sufficient to single-out or distinguish an individual from others. However, in a smaller setting, say in a classroom, a first name would suffice (Article 29 Data Protection Working Party, 2007).

Typically, identification is achieved through pieces of information, referred to as "identifiers", that relate to a particular individual (Article 29 Data Protection Working Party, 2007). Any information that reduces the uncertainty around the identity of an individual can be said to be an identifier. While some identifiers, such as a first or last name may not be sufficiently specific or may change over time, others such as fingerprints or genetic data are usually considered to be particularly good identifiers, since they can generally only be linked to a specific individual and are likely to stay constant through the lifetime of an individual.

The Supreme Court, in *Justice KS Puttaswamy (Retd.) v. Union of India (2017)* recognised that the right to privacy extends to an individual's identity, being tied to notions of autonomy, dignity, and self-determination.[6] The draft PDP Bill, 2019 builds on the jurisprudence laid down in Puttaswamy by seeking to protect "personal data", which it defines as "data about or relating to a natural person, who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall also include any inference drawn from such data for the purpose of profiling".[7] The definition is therefore extremely broad and includes any information that relates to an identifiable, living individual or indeed any information inferred from such information. Such personal data is therefore subject to privacy protections. The means of identification may be direct, as in the case of a unique identifier or a combination of two identifiers such as name and address; or may be indirect, such as when an IP address is combined with other data sets to lead to the specific identification of an individual.

In contrast, the term 'anonymity' is commonly recognised as being the opposite of identifiability, i.e. where the individual cannot be singled out or distinguished at all (Skopek, 2015).[8] The PDP Bill, 2019 treats "anonymised data" as the opposite of "personal data". A similar definitional approach has been adopted by the Report by the Committee of Experts on Non- Personal Data Governance Framework (the "NPD Report").[9] The 2017 Puttaswamy decision also notes Alan Westin's conception of "anonymity" as a "freedom from

[5] A person can generally be considered to be "identified" when he or she can be " 'distinguished' from from other members of a group" (Article 29 Data Protection Working Party, 2007) and (McCallister, Grance & Scarfone, 2010).

[6] Refer pages 85, 124, 252 of the majority judgment delivered by Chandrachud J., and pages 28, 30 of the concurring judgment authored by Sanjay Kishan Kaul J. in *Justice KS Puttaswamy (Retd.) v. Union of India (2017).*

[7] Clause 3(28), PDP Bill, 2019. In contrast, the draft Bill defines "de-identification" in Clause 3(16) as the process by which identifiers may be masked or removed from personal data.

[8] The word "anonymous" literally translates as "without name". However, in the current context, given that means of identification have grown beyond mere nomenclature, the term is used more broadly to refer to information that does not contain any data that can be directly or indirectly linked to an individual.

[9] The NPD Report defines anonymous data as "Data which is aggregated and to which certain data transformation techniques are applied, to the extent that individual specific events are no longer identifiable."

identification despite being in a public space." Writing for the majority, Chandrachud J. attempts to conceptually distinguish privacy and anonymity by stating that "privacy involves hiding information whereas anonymity involves hiding what makes it personal". As Skopek (2015) explains, consider a blood test result that is placed in a blank file, rather than the patient's medical file. If you gain access to the patient's medical file, but not her test result, then the patient's privacy (in respect of the results of her test) is protected. Conversely, if you access the test result, but not the medical file, the patient's anonymity is protected, since you will be unable to determine the identity of the patient from simply their test result.

Anonymised data is therefore that which has been treated so that it can no longer enable identification of an individual, directly or indirectly.[10] In this context it is important to reiterate, that as recognised by the Report of the Justice Srikrishna Committee, "data no longer exists in binary states of identifiable or non-identifiable" (Justice Srikrishna Committee, 2018). The degree of identifiability may be contextual, depending on the specific nature of the data, and the manner and method of processing thereof. Essentially, identification can, to a large extent, depend on the means and methods available to re-identify a data set (Justice Srikrishna Committee, 2018).[11] Anonymity can also be seen as contextual, in that in any single transaction, an individual may be anonymous to some while being identifiable to others. For instance, the general public may be unable to determine the real-world identity of the user of an pseudonymized social media account. However, as we discuss in further sections of this paper, the social media intermediary itself will usually be in a position to identify the user involved.

Establishing identity and enabling identification is critical to the functioning of human societies by enabling efficiencies in social transactions, allocation of social, legal and economic responsibility, targeting welfare functions, levying proportionate taxation, ensuring access to rights, etc. Equally, however, enabling or permitting anonymity can have numerous social benefits, as we explain next.

2.2 Understanding the case for the 'right' to online anonymity

The tension between the need of society to identify individuals, and in some cases to recognise the limits of identification have only been exacerbated by the Internet. As is commonly recognised, the ability to navigate the Internet relatively anonymously is one of the defining characteristics of the medium, even if the Internet was not, as such, designed to facilitate anonymity (Clark, 1988). Justifications for anonymity are typically based on the broader benefits it yields for individuals and society as a whole, particularly in the context of facilitating a thriving and strong democratic society. While anonymity may be counterproductive in certain contexts, understanding the importance of anonymity requires us to zoom out of an excessive focus on harms and accountability and adopt a deeper and more holistic perspective.

Online anonymity rests on similar normative foundations to the right to privacy itself. Consequently, much like the right to privacy, the 'right' to online anonymity cannot be an absolute right. However, in order to better understand the value and limits of any right to online anonymity, we have divided the arguments into three inter-related and intersecting considerations of speech, privacy, and equality.

[10] In theory, completely anonymised data should render an individual unidentifiable either when taken on its own, or in conjunction with other (unrelated) data sets. In practice, however, it appears this is difficult to do, with more and more research indicating the impracticality of full anonymization of personal data.

[11] As an example, one may refer to the Patrick Breyer case (*Patrick Breyer v. Bundesrepublik Deutschland (2016)*). Here, dynamic IP addresses were held to be personal data in certain contexts, as the digital media services provider who had access to the data subject's IP information, could identify the data subject with the assistance of other persons (state authorities and the internet service provider). The additional data sets (held by the state authorities and the ISP) were "likely reasonably to be used in order to identify the data subject". Whether in fact, such identification was done, was not relevant; merely the possibility that such identification was reasonably likely.

2.2.1 Speech-related benefits

There are various speech-related benefits to online anonymity. First, the right to anonymity, both in the online or offline context, enhances autonomy and dignity of individuals by allowing them to express themselves freely, without fear of retribution, harassment or reprisal (Skopek, 2015). Ensuring that individuals are not identified based on their speech is especially important in the case of unpopular, dissenting, or marginalised views.

Anonymity provides the necessary cover to activists and human rights defenders to voice their dissent against a hostile state, that is capable of using the strong arm of the law to threaten and silence them (Sharma & Qadir, 2020). Such an ability to freely dissent and critique the state furthers a deliberative democracy and enhances information flow to citizens regarding the activities of the state (Nair, 2019). Interestingly, anonymous speech was utilised as an effective way to debate critical public questions during the American independence movement. Alexander Hamilton, John Jay, and James Madison famously authored the Federalist Papers under the pseudonym Publius, and the revolutionary-era pamphleteers published under assumed names, often to escape prosecution (Boudin, 2011). Voltaire and Benjamin Franklin also wrote under assumed names (Daniyal, 2015). The U.S. Supreme Court has expressly observed that anonymous forms of speech had been *"historic weapons in the defense of liberty, as the pamphlets of Thomas Paine and others in our own history abundantly attest" (Lovell v. City of Griffin, 1938)*, and has thus extended its protection for members of threatened minorities and unpopular organisations *(NAACP v. Alabama, 1958)* .

These speech-related benefits of anonymity offline are also reflected in the online space. Indian Twitter is replete with anonymous parody accounts, such as PuNsTeR(TM) (Pun_Starr), ROFL Gandhi 2.0 (RoflGandhi_), Jawaharlal Nehru (PMNehru) and Pen Pencil (penpencildraw) that leverage their anonymity to engage in political satire and freely critique the socio-political culture in India today. The role played by online anonymity in modern democratic movements was evident during the pro-democracy protests in Hong Kong, where anonymity offered by encrypted platforms was utilized to mobilize protests, while the police used digital trails to track and punish protestors (Smith, 2019; Shao, 2019), although social media platforms were also used for misinformation campaigns (Keller, Schoch, Stier & Yang, 2019).

Second, and a related point, is the importance of anonymity for source protection. Democratic functioning relies on the contributions of journalists and whistleblowers, to hold the powerful to account. In this context, it is notable that whistleblowers for instance, do enjoy certain limited protections under Indian law (Bhatia, 2014).[12] The anonymity provided to whistleblowers can enable the revelation of important information in the public interest. This could occur for instance, in the citizen-state and employer-employee/ corporation-contractor contexts. For example, many healthcare workers used social media to disclose safety lapses and lack of protective gear in hospitals during the course of the COVID 19 pandemic and faced censure or even termination of employment as a consequence (Scheiber & Rosenthal, 2020; Carville, Court & Brown, 2020). In such situations, providing for anonymity over social media can ensure that critical public interest issues are disclosed, and that whistleblowers do not face government/ organisational reprisal.

[12] The Whistle Blowers Protection Act, 2014, ensures the protection of the identity of whistleblowers and contains norms against victimisation, but criminalises frivolous complaints and does not provide strong statutory enforcement mechanisms (Liu, 2014; Upadhyay, 2019).

The concerns that motivate protection of whistleblowers also animate the importance of source protection by journalists, in order to enable the 'watchdog' role played by the news media in a democracy.[13] However, Indian law does not adequately address these concerns of confidentiality, and when called upon to provide evidence before a court, journalists may be required to disclose their sources or face contempt proceedings (Mitta, 2012; Chatterjee, 2018). Generally speaking, Indian courts have used varying notions of 'public interest' to compel the disclosure of sources,[14] which is a direct consequence of the right to anonymity not being an absolute right. Overall, the right to source protection in India appears to be considered on a case-to-case basis, balancing the right of the media to free speech and its role in providing information to the public with the need to ensure proper administration of justice. Unfortunately, however, it appears that often, the latter tends to outweigh the former, especially since courts have refrained from considering the privacy interests of the source as a basis for ensuring their anonymity.

Third, online anonymity facilitates discussions on issues that are often considered taboo in society. In India, these could include discussions pertaining to sexuality, sex education, sexual violence, abuse, disease and gay marriage (Rigby, 1995; Matthan, 2019). It also enables individuals and groups to avoid source bias, permitting their ideas to be judged on their merits, rather than based on the identity, ideology, or popularity of the speaker (Boudin, 2011). The creation of a more diverse marketplace of ideas can be vital in a democratic society, where criticism of the prevailing social power dynamics may be essential for social progress. In doing so, online anonymity allows both "good" and "bad" minority opinions to thrive (Daniyal, 2015).

There is no question that anonymity can reduce accountability and encourage or exacerbate illegal or irresponsible speech, fake news, and hate speech, with women often bearing the brunt of such misogynistic anonymous 'troll' speech (Stoeffel, 2014; Seth, 2010; Rainie, Anderson & Albright, 2017). Anonymity makes it easier to indulge in behaviour that would otherwise be constrained by social mores, which have developed in the physical world precisely to prevent certain types of harmful behaviour (Citron, 2009). Given the disconnect between peoples online activity and their real life identity and the distance from the physical world, anonymity promotes 'deindividuation' that allows people to band together and act aggressively online and ignore real world consequences of one's actions. (Littleton, 2019). Thus, anonymous users do not feel the need to be "politically correct" or inhibit their "baser" feelings, which may lead to trolling of women, religious and sexual minorities, and dalits. Plato in The Republic, wrote about the Ring of Gyges, a mythical, magical ring that renders the wearer invisible. Using the powers of invisibility bestowed by the ring, a shepherd seduced the queen of Lydia and killed the king (Hartzog & Selinger, 2015). The Ring of Gyges is a parable for morality being a social construct, which vanishes the moment complete anonymity is granted; hence people operate on the assumption that they will not get caught for any violations of the law (Daniyal, 2015). Thus, Plato believed that without

[13] Accordingly, many jurisdictions recognise such a right in their laws. See for example, Section 10, UK Contempt of Court Act, 1981, Section 53(1), German Civil Procedure Code, Article 17(3), Swiss Federal Constitution, 1999. Also refer Human Rights Resolution 2005/38: The Right to Freedom of Opinion and Expression, E/CN.4/RES/2005/38;AfComHPR, Declaration of Principles on Freedom of Expression in Africa, Section XV. Also refer (Oster, 2015).

[14] For example, in *Javed Akhtar v. Lana Publishing Co. (1987)*, the court ordered disclosure of sources as the article in question dealt with the private lives of the plaintiff and his wife, which was held not to serve public interest. In Jai *Prakash Agarwal v. Vishambhar Dutt Sharma and Ors. (1986),* the Delhi High Court, while ordering disclosure of sources, noted that before doing so, courts should be convinced that this would be in public interest. In *Dr. S Krishna Rao v. Ushodaya Publications (2008)*, the Andhra Pradesh High Court made an interesting distinction by recognising that source protection could be permitted at the initial/interim stages of a case, but that such protection would not be available at later stages of trial. In re: *Resident Editor and Ors. Of the Hindustan Times (1989)*, the Patna High Court noted that the publication would have to be in 'public interest' in order to claim the benefit of source protection.

accountability, we would all behave in an unjust manner.[15]

Anonymity also heightens the perceived majority status of people online and allows the user to view the online interaction almost as a game, instead of an interaction involving a real person on the other side. This exacerbates the intensity of one's behaviour, termed as 'the online disinhibition effect', while reducing any blowback that an individual may receive if the victim was in the same physical space as them (Suler 2004, 3). By allowing people to evade identification and violate the privacy and dignity of others without consequence, online anonymity makes it extremely difficult to hold them accountable for their conduct (Solove, 2006; Davenport, 2002).

However, the solution to fake news, hate speech, and misogynistic speech is not to prohibit online anonymity. While anonymity may increase the volume of such speech, mandating identification and traceability will not shut it down. This is because the online disinhibition effect exists for *all* interactions online. The physical distance from the victim, the easy ability to dehumanise them, mob mentality, and the relative lack of any social, moral, or legal repercussions and accountability will continue to engender abuse online. In 2020, Amnesty International (2020) released a report, "Troll Patrol India", which documented the large scale abuse faced by Indian women politicians, particularly belonging to minority groups, even when the trolls were not anonymous. Outlawing anonymity will not simply halt the online abuse, even though it will increase the vulnerabilities of marginalised groups (Collins, 2015). Conversely, the possibility of online trolling and hate speech may actually be used to argue for the need for users to be able to hide their identities, particularly in the case of vulnerable or marginalised groups and individuals (Boudin, 2011).

As we have argued previously, a big part of the solution to the problem of hate speech, fake news, and sexist and misogynistic abuse online lies in improved implementation of existing laws, adopting a co-regulatory approach and other non-legal alternatives (Bailey & Bhandari, 2021).[16] In fact, empirical studies over a multiyear dataset of a social media platform have shown that identity verification by such platforms has not been effective in deterring the creation and sharing of fake news, and may instead incentivise malicious users to 'game' the verification system by creating fabricated identities (Wang, Pang & Pavlou, 2014). We also need to re-evaluate our approach to online content moderation to consider the best way to reduce online abuse (Langvardt, 2018).

Fourth, the critical function of enabling free speech performed by anonymity is recognised in our electoral processes through the secret ballot. The right to vote anonymously protects the freedom to vote, without any threat or repercussions or intimidation, thus allowing voters to reveal their true preference of candidates.[17] In India too, the secrecy of vote is guaranteed in case of national or state

[15] Hollywood too has seen an extension of this trope in movies such as Hollowman. Closer home, we have seen the powers of anonymity explored in the popular Hindi movie Mr. India. interestingly however, Hollywood focuses on the anonymity as a danger trope, while the Indian film sees the benefits of anonymity in enabling a rebalancing of power equations.

[16] Expert evidence introduced before the Madras High Court in the Anthony Clement Rubin case also suggests the adoption of more holistic and less intrusive alternatives (than building traceability into platforms). Suggestions include the need to improve education and information illiteracy as well as various technological measures that can be adopted by social media companies and fact checkers (Prabhakaran, 2019).

[17] The importance of the secret ballot "as an essential defining characteristic of any legitimate democratic system" is best captured by the Allahabad High Court in *Rekha Singh v. State of Uttar Pradesh, 2019* in the following words: *"The choice made in secrecy and privacy are essential features which determine the outcome of an independent choice exercised by the voter...The question to be addressed is not whether the choice while casting the vote was made on account of any coercion, threat or influence (all to be pleaded and established) but whether the choice was made with a free mind, free from perception of fear, coercion or influence. The foundation of any electoral process is the belief in secrecy and anonymity during voting process which two things have real impacts on the choices made during the electoral process. It is not only desirable that the*

assembly elections, and no person or witness can be required to disclose whom they have voted for in an election,[18] although this individual right to a secret ballot can be waived (Laxmi Singh v. Rekha Singh, 2020). Every official involved in the conduct of elections must maintain the secrecy of voting, except where required by law.

However, it is important to note that the right to anonymity in an electoral process does not take away from the verification procedure, such as through voter-verified paper audit trails (VVPAT) in India, which is necessary to ensures the accuracy and fairness of the elections. As Langer, Jonker and Pieters (2010) explain, anonymity ensures that no one can "link" a vote to a particular voter, while verifiability ensures that everyone can "link" the votes to the final election results.

We are not making a case for absolute anonymity in all situations in the online space - just as we recognise that one cannot have anonymity in all parts of the electoral or legislative process. For instance, there are many valid criticisms around the use of anonymous electoral bonds in election financing in India that, as critics have argued, have legitimised opacity and institutionalised political corruption (Vaishnav, 2019; Suchindran & Pandya, 2018). In fact, mandatory identification in certain cases, also aligns with democratic values that demand public disclosure and transparency, especially in a lawmaking or enforcement process (Boudin, 2011). Transparency in state action achieves important public oversight, and ensures accountability, whether by ensuring the public knows the the name of the sponsor of a legislative bill or the identity of the police officer who arrested an accused (Davenport, 2002). Transparency also underlies the traditional licensing or registration requirement for all services engaging in forms of public speech ranging from radio, broadcasting to cinema, which makes anonymity impossible, because they are considered to be engaging in public speech and not speech between individuals or small groups. It is, for instance, the same reason why secretive and anonymous speech by the press is considered a menace to society (*In re Galavandar v. Unknown, 1957*).

2.2.2 Privacy-related benefits

Apart from facilitating speech, the benefits of online anonymity can also be viewed through the prism of privacy it can provide to individuals and groups. First, anonymity enables experimentation with identities and opinions, and is particularly important for those living outside majoritarian social mores such as queer, transgender, and other marginalised groups such as sex workers or HIV-positive persons (Stein, 2003). In 2017, India enacted the HIV and AIDS (Prevention and Control) Act, 2017, which expressly recognised the need for anonymity of HIV positive persons in the offline context. The law requires the anonymity of "protected persons" to be maintained in any court proceedings involving them.[19] Courts are also empowered, 'in the interests of justice', to direct proceedings to be carried out in-camera and to restrain any reporting/publishing of information that may lead to disclosure of the name, status or identity of the protected person.

A related benefit of anonymity is that it helps persons existing on the margins of society to be invisible to the State and avoid some of the power differentials and associated violence that are present offline (Kovacs, 2020). Anonymity not only protects against discrimination, but it can also save lives. As Human Rights Watch observes, the ability to speak anonymously is essential for "human rights defenders, journalists, and vulnerable minority groups." In his 2015 Report, the United Nations Special

actual secrecy during the voting process must be maintained, it is in fact the duty of the functionaries conducting the elections to strengthen the 'perception of ballot secrecy'."

[18] Sections 94 and 128, Representation of People Act, 1951. It is worth noting, however, that while voting for the Lok Sabha (the House of the People) is done through a secret ballot (except in cases of voting by proxy), seats are filled in the Rajya Sabha (the Council of States) through an open ballot. See Sections 59 and 60, Representation of People Act, 1951.

Rapporteur, David Kaye, highlighted the importance of anonymity and encryption in creating a "zone of privacy" which facilitates private communication, and serves as a shield in hostile political, religious, and social environments (Kaye, 2015). We saw this in India as well, when in 2015 a local journalist in Uttar Pradesh, Jagendra Singh, was murdered allegedly in response to his Facebook post identifying a minister's involvement in illegal mining and land grabbing (PTI, 2015). Had his identity remained anonymous, this may have been prevented.

The privacy benefits of anonymity apply against private individuals in a similar manner. For instance, anonymity allows an individual to keep their whereabouts secret from a former partner or family member or to keep information about their access to counselling or health services private. This is not a mere hypothetical concern. A year after the National AIDS Control Organisation (NACO) required all patients receiving the life-saving Antiretroviral Therapy to link these services with Aadhaar, more than 50% of the targeted vulnerable population failed to comply with the order - and risked losing access to ART - because of the fear of stigma and discrimination on being identified in public (Surakha P, 2017).

Next, anonymity is recognised in certain contexts in the judicial process and courts have recognised the importance of suppressing the identity of parties in cases where the disclosure of certain facts during the course of proceedings could lead to harassment, social ostracism, discrimination or similar consequences for the parties. For instance, in *Mx of Bombay Indian Inhabitant v. Zy (1997)*, the Bombay High Court held that it could always permit an HIV infected party to suppress their identity at the appropriate stage and "in proper cases and in the interests of administration of justice".[20] However, since the right of anonymity is not absolute, it has to be balanced against other equally important or even overriding interests. Thus, although patients are entitled to their privacy, courts have held that doctors are permitted to make relevant disclosures in public interest, such as where there was an "immediate or future health risk to others". In *Patient X v Hospital Z (1998)*, the Supreme Court was considering whether a doctor had the right to inform a person's fiance of their HIV positive status, and the Court held that the right to patient privacy was not absolute, and would be subject to "such action as may be lawfully taken for the prevention of Crime or disorder or protection of health or morals or protection of rights and freedoms of others."

Similarly, the need for anonymity for victims of sexual assault and rape has been built into the law, both in the civil[21] and criminal sphere,[22] and by adopting the principle of an *in camera* trial in cases of rape[23] or

[19] A "protected person" is defined in Section 2(s) of the HIV/AIDS Act as an HIV positive person, or a person who is or has lived/resided/cohabited with a person who is or was HIV positive. Per Section 34 of the HIV/AIDS Act, a court may, on application by the protected person, allow suppression of the identity of the protected person by substituting their name in court proceedings with a pseudonym

[20] Noting that such a decision would depend on the facts of the case, the Court approved of a process where a suit would first be filed indicating the parties identities, which could then be suppressed at a later stage upon moving an appropriate application before the court.

[21] The Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 prohibits the publication of the identity and addresses of the parties / witnesses in a sexual harassment matter.

[22] Section 228A of the Indian Penal Code criminalises the disclosure of the name of "any matter which may make known the identity" of victims of sexual offences such as rape and gangrape with a punishment of up to two years. The law provides for certain exceptions, such as when the victim (or her next of kin, if she is dead or a minor or of unsound mind) waives the right of anonymity, or when the identity is disclosed in good faith by the police during the course of investigation. In *Nipun Saxena v. Union of India and Ors (2019)*, the Supreme Court expressed certain apprehensions about the fact that Section 228(2) could be misused in cases where the interest of the "next of kin" of the victim may diverge from the victim, such as in cases of rape by a member of the family. It also expressed its discomfort with taking away the agency of an unsound person.

[23] See, for instance, Section 327(2), Cr.P.C., 1973

where it is "clearly and necessarily" required in the interests of justice dispensation *(Naresh Shridhar Mirajkar v. State of Maharashtra, 1966).* The rationale behind guaranteeing anonymity to victims of such crimes is to protect them from hostile discrimination, social ostracisation, and harassment *(Nipun Saxena v. Union of India and Ors, 2019)*; and also to safeguard their right to privacy and insulate them from "unnecessary public comments" *(Aju Varghese v. State of Kerala, 2018)*. Anonymity is achieved by prohibiting the publication of the name of the victim, as well as any other identifying information, such as the name of their relatives, school, and village.

These considerations apply with even greater force in the case of children given their special and vulnerable status. Thus law in general, prohibits the disclosure of the identity of children who are in "conflict with the law", i.e. they are accused of committing an offence; or are children "in need of care and protection";[24] child witnesses; and child victims of sexual assault or harassment (unless it is considered in the interest of the child by the Special Court).[25]

The law thus aims to protect victims of sexual harassment and sexual assault from the ill-effects of publicity pertaining to sexual abuse, thereby encouraging women to initiate legal action where appropriate, and protecting them from social opprobrium; while also ensuring that witnesses are protected from possible attempts to influence them. During the #MeToo movement, anonymity served a speech and privacy benefit, by providing the necessary protection to help women speak against sexual harassment by powerful men in art, entertainment, politics, and the media. However, courts in India have often undermined this protection in cases dealing with anonymous sexual harassment allegations made during the #MeToo movement. For instance, the Instagram account 'herdsceneand' collected and published various anonymous sexual harassment allegations against artists Subodh Gupta and Riyas Komu. In response, Subodh Gupta filed a defamation suit against'herdsceneand', arguing that the anonymous nature of the allegations had made it impossible for him to respond and issue specific denials, thereby sullying his reputation. During the course of the hearing, ordering the take down of various media reports carrying stories about the anonymous allegations, the Delhi High Court noted, "prima facie, it appears that the allegations as made in the allegedly defamatory contents, cannot be permitted to be made in public domain/published without being backed by legal recourse. The same if permitted, is capable of mischief."[26] Eventually, in view of a compromise executed between the parties, Instagram did not end up having to reveal the identity of the owners of the account 'herdsceneand'. The observations by the High Court are not limited to cases involving sexual harassment and have been extended to anonymous and allegedly defamatory allegations regarding investments and business dealings, where the Delhi High Court directed the permanent blocking and disabling of a defamatory URL, stating:

> "….Though the impugned contents are found to be in the nature of a whistle blower but it is felt that when the publisher thereof is not even willing to disclose the identity, such malicious campaign should not be permitted….
>
> …I have in Subodh Gupta Vs. Herdsceneand MANU/DE/3168/2019 also observed that without the accuser identifying himself/herself, allegations in the public domain cannot be permitted to be made without being backed by legal recourse, and the same, if permitted, is capable of mischief….I have held that none can be condemned publicly, without having an opportunity to defend him/herself."[27]

[24] Section 74, Juvenile Justice (Care and Protection of Children) Act, 2015. If the Juvenile Justice Board or Committee is of the view, expressed in writing, that the disclosure of identity would be in the "best interest of the child", they may authorise such disclosure. Identity in these cases involves the name, address, school, and other particulars which may lead to the identification of the child. See also Subash Chandra Rai v. State of Sikkim, (2018) SCC Online Sikk 29.

[25] Sections 23, 24(5) and 33(7), POCSO, 2012.

[26] See order dated 21.01.2020 passed by the Delhi High Court in (Subodh Gupta v. Herdscene and Ors., 2019).

By taking a dim view of anonymous allegations in both these case, the Delhi High Court, unfortunately, ignored the patriarchal power structures and numerous social, legal, and professional barriers that discouraged women from reporting sexual harassment allegations (Bhandari & Kovacs, 2021). As Dasgupta (2019) notes, the #MeToo movement in India gave a new language to Indian women to cultivate solidarity and speak out against abuse. Anonymity online protected them from the social, financial, physical, and legal retaliation that may be the cost of speaking out (Jayawardane, 2019), but the decisions of the Court forced them to choose between their privacy (by revealing their identity) or their right to tell their story.

Finally, anonymity can make it easier for individuals to interact with one another in many contexts. Considerable research has been done on the concept of the 'anonymity of a stranger', and how this can help individuals express themselves without fear of repercussion. This may be required in various contexts, for instance in accessing counselling, reproductive health services, or domestic violence related services (Kang, Dabbish & Sutton, 2016).

2.2.3 Equality-related benefits

Under certain conditions, anonymity helps individuals shield themselves from the power of private corporations and the state by remedying the asymmetric nature of the relationship. The steady deployment of profiling and surveillance technologies by private and state actors in all our online interactions aided by the advancements in data mining, has heralded a world of surveillance capitalism (Froomkin, 2017).

The rapid deployment of profiling and surveillance technologies in both the public and private sectors only increases the importance of preserving the ability to be anonymous: without it, every utterance, every purchase, every computer-mediated interaction risks becoming part of one's profile.

First, in a world where both private collection and analysis of personal data is on the rise, online anonymity enables individuals to exercise greater control over their personal information and decide how much personal information will be shared or revealed to others. Users can utilise online anonymity to avoid large scale data collection and targeted and/or direct marketing (or even manipulation) by private companies (Davenport, 2002). However, in practice, as we detail later, in a world marked by online transactions, it is very difficult to achieve anonymity from private corporations, and it is much easier and more reasonable to expect a user to achieve platform anonymity (vis-a-vis other users on the platform), rather than customer anonymity (vis-a-vis the intermediary) (Zingales, 2018).

In fact, law enforcement agencies support mandatory identification mechanisms on the ground that it aids investigation and prosecution of those engaged in the commission of online offenses such as hate speech, sale or advertisement of regulated goods and services, infringement of intellectual property rights etc. Consequently, Reddy (2018) argues that governments are entitled to demand traceability and identification even from encrypted online messaging platforms such as Whatsapp and Signal, which allow their users to engage in anonymous public speech through forwards and participation in groups. Similar claims have led to a restriction on anonymity in the financial sector in India. Notably, the recommendations of the Financial Action Task Force (FATF), which form the basis of the Indian Know-Your-Customer (KYC) framework, contain a blanket prohibition on the use of anonymous accounts. It is believed anonymous accounts enhance the risk of money laundering or terrorist financing. Identity

[27] Sunil Sachdeva vs Owner Of Domain Name www.Cjr7.Com, CS (OS) 385/2019, order dated 13.11.2019 (Delhi High Court).

verification protocols form a critical part of the FATFs recommendations, as this is seen as vital in enabling the detection of suspicious customers and transactions.[28] However, the privacy and other costs of this mandate are also increasingly being recognised (Bailey, Bhandari & Goyal, 2021; Bailey, Sane, Goyal & Varma, 2021).

We have previously argued that a certain element of friction must be present in the law enforcement functions of the State, much like due process guarantees (Bailey, Bhandari & Rahman, 2021). The use of encryption online for instance can help prevent mass surveillance (Bailey, Bhandari & Rahman, 2021). Anonymity plays a similar role – by allowing individuals to express critical or unpopular views or access censored content online, anonymity can act to protect a range of human rights. At the same time, it only makes it difficult, but not impossible for law enforcement agencies to trace the identity of a person. Technical means such as IP addresses and cookies, as well as other demographic details that may be provided or automatically collected by the social media platforms provide avenues for law enforcement to identify an individual (Froomkin, 2017). In fact, the advancements in surveillance technology, whether facial recognition, gait analysis or CCTV usage make it even more important that anonymity provide a check against mindless data collection (Evans, 2014).

The arguments elaborated in this section emphasise the complex nature of online anonymity. As Matthan (2019) notes, anonymity simultaneously allows trouble makers to "hide in plain sight", while also providing necessary protection "to those who need their identity masked." Therefore removing the ability to engage anonymously or/and pseudonymously online will have a chilling effect on freedom of expression, erode individual and group privacy, and may even endanger the safety of individuals or marginalised groups.

Based on the arguments above, we believe that it is necessary to recognise a right to online anonymity and the right to receive and communicate information anonymously online as part of the right to free speech and expression and privacy under Articles 19(1)(a) and 21 of the Constitution. Such a right to online anonymity will not be absolute. However, as we shall elaborate in the next section, any restriction on such right should meet the proportionality standard articulated in *Justice KS Puttaswamy (Retd.) v. Union of India (2017) and Justice KS Puttaswamy (Retd.) v. Union of India (2019).* Thus, compelled disclosure of an anonymous speaker must be justified on the basis of a law, must be suitable or rationally connected to a legitimate state aim, must be necessary, adequately balance competing interests, and have sufficient procedural guarantees to ensure that it is not abused.

3. Online identification mandate and emerging constitutional concerns

In this section, we use the arguments pertaining to anonymity discussed previously, to highlight the constitutional concerns emanating from regulatory proposals that seek to limit anonymity by requiring identification of users on social media platforms. To this end, we examine two rules in the recently notified Intermediary Liability Rules, 2021 that aim to facilitate identification of users of large social media platforms. These are: (i) Rule 4(7) of the Intermediary Liability Rules, 2021 that requires

[28] RBI, Master Direction: Know Your Customer Direction 2016, updated on 18.12.2020, RBI/DBR/2015-16/18, https://www.rbi.org.in/CommonPerson/english/scripts/notification.aspx?id=2607.

significant social media intermediaries[29] to enable voluntary verification of user accounts, and (ii) Rule 4(2), of the Intermediary Liability Rules, 2021 that imposes an obligation on significant social media intermediaries that provide messaging services, to enable traceability of the first originator of information on their platforms.

3.1 Removal of online anonymity and constitutional concerns

As mentioned previously, the *Justice KS Puttaswamy (Retd.) v. Union of India (2017)* case recognized that the fundamental right to privacy flows from the rights guaranteed under Part III of the Indian Constitution. Thus, the claim of online anonymity rests on a similar normative basis as the right to privacy. Given that the right to privacy is itself not an absolute right, the right to anonymity also cannot be absolute, and can be subject to restrictions as permissible under Article 14, 19, 21 of the Constitution. Therefore, any interference that requires the removal of anonymity of individuals on a platform will have to meet various constitutional requirements laid down by the Supreme Court in *Justice KS Puttaswamy (Retd.) v. Union of India (2017).* Per the Supreme Court, the validity of any restrictions imposed by the State on the right to privacy has to be tested using the necessity and proportionality standard. This involves scrutinising a law using the tests of legality, legitimate aim, proportionality and procedural safeguards. In 2018, in the Aadhaar judgment in *Justice KS Puttaswamy (Retd.) v. Union of India (2019),* the Supreme Court elaborated upon this standard and framed tests that would form a part of the proportionality analysis undertaken by courts (Bhandari & Lahiri, 2020; Parsheera & Bailey, 2018). In accordance with the decision in both these cases, *any* restriction into the right to privacy has to be subjected to the following tests:

- *Legality:* Does the restriction emanate from a law?
- *Legitimate aim:* Does the restriction pursue a legitimate State aim?
- *Suitability:* Do the means adopted by the restriction bear a rational nexus to the stated objective of the restriction?
- *Necessity:* What alternatives can be identified and are these as effective as the chosen restriction in achieving the stated end? Is there any way of achieving the same objective which will be less intrusive on the fundamental right to privacy?
- *Proportionality:* Is the interference into the right to privacy proportionate to the need for such interference, i.e do the benefits of the restriction outweigh the costs of the intrusion into the right to privacy? Further, within the proportionality analysis, courts also invariably calibrate if impugned state action or law sets out adequate procedural safeguards to protect against abuse.[30]

We discuss how these tests could apply to the Intermediary Liability Rules, 2021 below.

3.1.1 Voluntary verification by 'Significant Social Media Intermediaries'

While India does not currently impose a legal requirement for users of online platforms to provide their real-name to the platform, Rule 4(7) of the Intermediary Liability Rules, 2021 states that significant

[29] "Social media intermediaries" are defined as those that primarily or solely enable online interaction between two or more users, and allow them to create, upload, share, disseminate, modify of access information using its services. To qualify as a "significant" social media intermediary, the platform must meet the user threshold specified by the government, which is currently 50 lakhs. Note that the Intermediary Liability Rules, 2021 also empower the government to notify any other intermediaries to comply with the obligations imposed on significant social media intermediaries, should certain conditions be met.

[30] See Justice Kaul's opinion in Justice KS Puttaswamy (Retd.) v. Union of India (2017).

social media intermediaries are under an obligation to enable Indian users to voluntarily verify their accounts by using any appropriate mechanism, including the active Indian mobile number of such users. The intent of such a provision is to enable users to assert their identities in the online space thereby promoting reliability and trust. Such a requirement could also help combat illicit activity such as identity theft and help restrict the spread of fake news, etc. That said, there are a number of concerns that stem from this provision.

First, even though the Intermediary Liability Rules, 2021 clearly state that intermediaries shall offer verification services on a voluntary basis, experience in relation to previous supposedly *voluntary* identification requirements indicates that often, these become de facto mandatory. For instance, both the Aadhaar ID as well as initiatives such as the Aarogya Setu app, despite purportedly being voluntary in nature, were virtually mandatory to access a variety of often essential services (Bhandari & Rahman, 2020; Bailey, Bhandari & Goyal, 2021). Such a mission creep is often done indirectly, by making access to critical services contingent on conforming with the requirement or removing the ability to provide alternative IDs (Bhandari & Rahman, 2020; Bailey, Bhandari & Goyal, 2021).

Expansion of a voluntary identity requirement into a mandatory requirement would essentially imply adoption of a real-name verification system by significant social media intermediaries. However, such a mandate may not actually promote greater online safety. Further, as discussed in the previous section, such a requirement could significantly restrict speech and privacy rights, and also promote exclusions/digital divide.

As mentioned previously, studies have demonstrated that identity verification is not necessarily an effective tool in deterring the sharing of illicit online content (Wang et al., 2014).[31] International precedent too largely favours avoiding mandatory real-name identification laws. China appears to be an exception in that it has implemented a real-name / mobile number verification system for access to social media (Xinhua News Agency, 2017).[32] In contrast, South Korean constitutional courts have struck down a law requiring large intermediaries (based on user numbers) to seek a user's Resident Registration Numbers (a 13 digit unique number assigned to every citizen at birth) at the time of registration for use of their services (Anonymous, 2021; Sang-Hun, 2012). In reaching its conclusion, the court noted in particular that evidence suggested that there was no change in the quality of online interactions, thereby indicating ineffectiveness of the law. Also alternative methods were available to intermediaries to deal with offensive online behaviour, in addition to which authorities could always access IP related data from them (Anonymous, 2021).[33] It was accordingly held that the benefits of the law were suspect, and outweighed by the costs (Sang-Hun, 2012).[34] Brazil represents an interesting case given that the Brazilian Marco Civil da Internet (the Internet Bill of Rights) explicitly forbids online anonymity. However in a notable ruling, pertaining to the blocking of the Sarahah app (that permitted anonymous user interaction), courts overturned the ban imposed by the State, holding that alternate methods existed to trace users of the app (including through retained user logs), and that the app was in essence similar to all others which did not implement an enforceable real-name policy

[31] One study on the effect of South Korea's real-name identification law however does point to how identification laws may not lead to a decrease in overall quantity of information being posted, and that quality of discourse did improve as a result of such laws (Cho, 2011). However, in addition to other limitations, the study does not specifically undertake an examination of the costs of the law, as it focuses primarily on correlating the drop in illicit language with the identification norm.

[32] This is done under China Cybersecurity Law of 2017, which also places restrictions on how such information can be used (Xinhua News Agency, 2017).

[33] An additional unintentional consequence of the law was that users from Korea were shifting to foreign-based online platforms (Sang-Hun, 2012; Anonymous, 2021).

[34] The court recognised that online anonymity confers several benefits, and that the negative effects thereof should be met through other less restrictive means that do not violate the possibility of anonymity altogether (Blagdon, 2012).

(Silva & e Fernanda Cohen, 2017). Previous case law in Brazil had noted that intermediaries must ensure that it provides resources towards "curbing anonymity and assigning each event a certain authorship". (Souza & Lemos, n.d.) Thus, the courts in Brazil appear to have distinguished between concepts of complete anonymity and 'apparent' anonymity. Complete anonymity - where a user cannot be traced at all, may not be permitted. However, platforms providing a service that promotes anonymous expression are free to do so, subject to there being other methods available to law enforcement to trace users, if so required.[35]

Second, it is unclear how significant social media intermediaries will engage in the process of voluntary verification or which documents they will seek to identify users, and whether any particular method used could be challenged as being inadequate or inappropriate. Indeed, the type of ID required by platforms will become a critical issue, not least due to concerns pertaining to robustness of many identification proofs commonly used in India or the ability of many, particularly minors, to access such identity proofs. Poorly designed identity requirements could therefore lead to exclusions and promote a digital divide, particularly of groups such as minors and the marginalised. One may note that imposition of onerous know your customer obligations in the financial sector, have been seen as contributing towards exclusions from the formal financial sector (Bailey, Sane et al., 2021).

Third, while the Intermediary Liability Rules, 2021 themselves permit the usage of phone numbers by intermediaries for verification, platforms such as Twitter currently already assign the verified account status based on a determination that an account is "authentic, notable and active". Among other things, a Twitter user can choose to submit a valid government issued identification such as passport or driver's license to seek a verified status on the platform (Twitter Help, 2021).

If significant social media entities seek the submission of any government issued identity document such as passport, voter identity or driver's license, they will be accessing and storing sensitive personal data such as official identifiers.[36] This leads to concerns regarding data retention as well as data security. In the absence of a strong data protection law, it could be a cause for concern that the collection and processing of such sensitive personal data could take place without the oversight of an expert regulatory body such as the Data Protection Authority envisaged under the Personal Data Protection Bill, 2019 (Internet Freedom Foundation, 2021).

Finally, it is questionable whether intermediaries will be in a position to scrutinise and authenticate identity data in any meaningful manner. In the absence of any such system, a verification scheme could be easily gamed, thereby defeating its purpose. It is commonly recognised that many identification methods in India are insufficiently robust. Indeed this was one of the reasons for the introduction of the biometric based Aadhaar system. However, even this has been shown as suffering from identification failures.[37] Even assuming Aadhaar to be sufficiently robust, and if therefore voluntary submission of Aadhaar details is sought for the purpose of verification, this will raise constitutional concerns regarding the use of Aadhaar details by private entities.[38] Despite two judgments by the Supreme Court around the right to privacy and the constitutionality of the Aadhaar project, there is a

[35] Note that more recently, Brazil is debating a (much criticised) fake news related law that enables platforms to request identification of users, requires mandatory retention of viral messages and user identity data, etc (Araujo & Gaudiot, 2020).

[36] Section 3 (26) of the Personal Data Protection Bill, 2019 defines "official identifier" as "any number, code, or other identifier, assigned to a data principal under a law made by Parliament or any State Legislature which may be used for the purpose of verifying the identity of a data principal". Further Section 3(36) categorises official identifiers as sensitive personal data.

[37] See for instance Sircar and Sachdev (2020) and (Somanchi, 2018).

[38] Given that many online intermediaries and social media companies may not be based in India, regulating their use of the Aadhaar ecosystem may also prove problematic.

lack of clarity about whether private entities are permitted to use Aadhaar authentication for identification of consumers as part of private services or products at all.[39]

Given first, that the Aadhaar decision made it clear that the use of such systems by the private sector impermissibly facilitated the"commercial exploitation of an individual biometric and demographic information by the private entities"; second, that decision did not specifically approve of private sector use of Aadhaar; and third, due to the fact that Aadhaar can only be used where the individual is accessing a service, subsidy or benefit provided by the State, we believe that a de facto requirement for use of Aadhaar authentication by social media intermediaries would be unconstitutional.[40]

In any event, given the unsettled nature of these interpretations, we believe that significant social media intermediaries should definitely not seek (or be required to seek) the submission of Aadhaar details from users for voluntary verification under Rule 4(7) of the Intermediary Liability Rules, 2021 before the broader issue of whether private sector entities are indeed permitted to use Aadhaar based authentication is resolved.

Overall, while the voluntary verification requirement may not in its current form, be considered unconstitutional per se, it could indeed be seen as problematic for reasons ranging from the absence of robust identification mechanisms, to the greater risk it subjects to users to. An expansion of the voluntariness of the mandate to an obligation to verify, would however likely be unconstitutional, particularly if linkages with Aadhaar are required.

3.1.2 The proportionality doctrine and the new traceability obligations

Rule 4(2) of the Intermediary Liability Rules, 2021 states that *"a significant social media intermediary providing services primarily in the nature of messaging shall enable the identification of the first originator of the information on its computer resource as may be required by a judicial order passed by a court of competent jurisdiction or an order passed under section 69 by the Competent Authority as per the Information Technology (Procedure and Safeguards for interception, monitoring and decryption of information) Rules, 2009…".*[41] This provision essentially means that messaging platforms such as WhatsApp, Telegram, Line, Viber, Signal etc., who provide end-to-end encrypted messaging services (and have the requisite number of users in India) will have to ensure that all content on their platforms can be linked with the first-originator. While the rule does not impose the need to remove anonymity within a platform's ecosystem (so for instance,

[39] There are two perspectives on the constitutionality of the use of Aadhaar authentication by private entities. Some argue that the majority of the judges in the Aadhaar verdict did not prohibit the use of Aadhaar based authentication by private entities per se, but required that such use be authorised by a law and satisfy the proportionality standard (Jain, 2018). On the other hand, some point to how even a legislation cannot permit private entities to use Aadhaar authentication, whether voluntary or not (Sebastian & Sen, 2020; Bhandari & Narayan, 2018; Prasanna, n.d.).

[40] Given this divergence in interpretation of the Justice KS Puttaswamy (Retd.) v. Union of India (2019) case, the amendments to the Prevention of Money Laundering Act (that seek to mandate linking of Aadhaar with bank accounts) have been challenged before the Supreme Court as constitutionally impermissible and against the (perceived) express prohibition on the use of Aadhaar by private entities in Justice KS Puttaswamy (Retd.) v. Union of India (2019).

[41] The rule is subject to various provisos that (a) limit the grounds on which such an order can be passed to the prevention/detection/investigation/prosecution/punishment of offences related to the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, or public order, or of incitement to an offence relating to the aforesaid, or in relation to serious sexual offences, (b) require less intrusive means to be considered before such an order is passed, (c) specify that the contents of the message shall not be disclosed under such an order.

users can still be permitted to use pseudonyms), it does require that all communications on a messaging service must be linked to the creator thereof.

In a petition filed before the Delhi High Court challenging the constitutionality of Rule 4(2), WhatsApp claims that this obligation will require it to break the end-to-end encryption used on its service, thereby affecting the privacy of all data sent on its platform by all users, forever (Mathi, 2021b).

In relation to the traceability obligation the burden will be on the State to demonstrate that this is backed by an appropriately formulated law (that is not vague, etc.) and that such a law pursues a legitimate state aim. Further, the government will have to demonstrate that imposing the traceability obligation on significant social media intermediaries is directly linked to and is, in fact, necessary to achieve such identified aim. In order to pass the subsequent tests of suitability and necessity, the State will have to show the different alternatives considered by it, and why imposing the traceability obligation was the only way to achieve the objective while engaging in minimum intrusion into the right to privacy and anonymity. Lastly, the government will have to establish that the benefits gained from imposing this obligation outweigh the net loss of privacy, free speech and anonymity incurred by messaging service users and that it has placed appropriate procedural safeguards to ensure that risks to individual privacy are minimised.

Insofar as the first test of legality is concerned, being contained in a government notification, the obligation can indeed be considered to be imposed by a law. A separate question does however arise regarding whether or not the Intermediary Liability Rules, 2021 are the appropriate method for imposing such obligations on intermediaries.[42]

The government has stated that the main aim of these obligations is "prevention, investigation, punishment etc. of inter alia an offence relating to sovereignty, integrity and security of India, public order incitement to an offence relating to rape, sexually explicit material or child sexual abuse material punishable with imprisonment for not less than five years."[43] The plurality opinion in *Justice KS Puttaswamy (Retd.) v. Union of India (2017)* has indeed held that these grounds can be used by the state for the purposes of crafting legitimate restrictions on the right to privacy. Therefore, the state may be able to establish that these rules pursue a legitimate aim.[44]

However, the outcome may not be favourable when it comes to the other tests under the proportionality analysis. For instance, Rule 4(2) will likely not pass either the tests of the unavailability of alternative options or the test of proportionality, i.e where the state has to show that the benefits of the restriction outweigh the costs of the intrusion it causes into the right to privacy (Chandra, 2020).

As far as the proportionality analysis is concerned, reports indicate that WhatsApp will soon have over 500 million users from India. End-to-end encrypted messaging apps such Signal and Telegram have recently also seen a major spike in their Indian user base (Ahmed, 2021). The government has not yet been able to establish satisfactorily if there is a way to ensure traceability without sacrificing end-to-end

[42] We have previously argued that the imposition of such new and substantive obligations, which are not contemplated in the parent Act, exceeds the scope of permissible delegated legislation. Such obligations can only be introduced through statutory amendment or enactment of a new law (Bailey, Parsheera & Rahman, 2019).

[43] Proviso to Rule 4(2) of the Intermediary Liability Rules, 2021. See also (Ministry of Electronics and IT, 2021)

[44] While one may also question the ambiguity in and possible misuse of broad terms such as "offences relating to sovereignty and integrity of India", or "public order" (particularly where the powers under the provision can be used ex-ante i.e. before occurrence of any offence), typically such phrases will come to be defined/limited through court dicta.

encryption which prevents the intermediary from reading the message. Therefore it is, unclear how traceability could be achieved as a standard feature without breaking end-to-end encryption. Thus, imposing traceability obligations on significant social media intermediaries such as Whatsapp, Signal, Telegram etc. could mean that such platforms will have to do away with end-to-end encryption altogether. Of course, this rests on the assumption that traceability of users is not technically incompatible with end-to-end encryption, which the literature is nearly universal in agreeing with (Bailey, Bhandari & Rahman, 2021; Mathi, 2021a; Barik, 2021).

Given the user base of these messaging apps, such an obligation is likely to impact millions of Indians who use these messaging applications on a daily basis. This requirement will therefore compromise the right to privacy and free speech of *all these individuals*, by stripping them of their anonymity on the Internet, identifying them to the messaging platform at all times, regardless of their conduct and in the absence of any evidence against them (Bailey, Bhandari & Rahman, 2021). It will therefore be incumbent on the state to prove, through data it has gathered, that the presence of online anonymity and encryption has actually resulted in increase in crimes and inhibited investigation, and to what extent.[45]

The knowledge that no personal communication is private from the messaging platforms and is always at risk of being traced by the government will also cause a chilling effect on individual behavior online. Such an obligation poses particularly high risks to journalists, researchers, activists and political opponents who fear retribution and surveillance from the government. Further, researchers and journalists working on issues that highlight or critique the functioning of these large technology corporations and the services they provide will undoubtedly also be under a disproportionate risk of being surveilled and censored by these platforms. The problems associated with a surveillance state are well recognised (including by the Supreme Court in the Aadhaar judgment). The ability of the government to trace any information on such platforms can be seen as a step in this direction.

A key aspect of the proportionality analysis involves a consideration of the impact or costs on other interests and rights. Should traceability and identification of individuals be possible, without any attempts to weaken or break end to end encryption, this may indeed be constitutional. However, as we argue in Bailey, Bhandari and Rahman (2021) a mandate to create systemic weaknesses in platforms would not be constitutional, particularly where a vast majority of users on these platforms are not engaged in illegal activities.

Further, within the proportionality analysis, courts also invariably calibrate if impugned state action or law sets out adequate procedural safeguards to protect against abuse. Interestingly however, Rule 4(2) of the Intermediary Liability Rules, 2021 say that traceability order can be passed by a court of competent jurisdiction or through an order passed under section 69 by the Competent Authority as per the Information Technology (Procedure and Safeguards for interception, monitoring and decryption of information) Rules, 2009.

However, as we discuss in Bailey et al. (2018), activities such as mandating surveillance over individuals are highly "discretionary", and require a complex balancing of various competing interests, in addition to which, the sheer number of such decisions, makes it virtually impossible to sufficiently scrutinise all cases with due rigour. Such activities are both difficult to automate and very difficult to deliver effectively. The scrutiny required on a traceability order is of similar nature as on an order for

[45] As we point out in Bailey, Bhandari and Rahman (2021), this should ideally include a deeper cost-benefit analysis that also includes state led evidence to demonstrate the number and type of offences that have risen due to encryption, the nature of hurdles it has created with respect to investigation etc.

surveillance. The nature of such a function is undoubtedly discretionary in nature, demands specific application of mind to the nuance of each case, and is transaction-intensive, due to the high volume of traceability requests that will likely have to be scrutinised by such individuals. In such a situation, judges are the most well placed to adequately balance the pursuit of civil liberties on one hand and calibrate the requirements of the state on the other (Bailey et al., 2018). Accordingly, the procedural safeguards set out in the Intermediary Liability Rules are inadequate to satisfy the proportionality standard laid down by the SupremeCourt in Justice KS Puttaswamy (Retd.) v. Union of India (2017).

Insofar as the presence of alternative methods of enabling traceability are concerned, two arguments may be advanced. First, most intermediaries, and particularly large platforms in the content layer often collect detailed and sufficient quantities of personal data to enable identification of users, which is already accessible to law enforcement. Intermediaries at the network and access layers also collect identification information in the course of service provision due to the Internet's design and hierarchical nature. Second, access layer related laws in India mandate identification of users and linkages to a real-world identity. All this data is accessible to law enforcement per current laws, as we discuss below.

Identity data collected by platforms:
It is clear that a large proportion, if not all commonly used online platforms collect different types of identification information of users. This may be a result of technical needs (in the case of say, IP addresses which are required for addressing), while tools such as cookies are frequently used to customise platform experience.[46] Indeed, the business models of large technology platforms are predicated on collecting and being able to identify users (and thereafter use this data, including for purposes such as targeted advertising or customisation of services). This is indeed why global conversations around the need for modern data protection laws have become the norm over the last decade.

Table 1 below provides an overview of the type of identification information that is collected by some major platforms in India, at the time of sign-up to their services and during the course of provision of services, as stated in their terms and conditions/privacy policies.

	Platform	**ID information at time of sign-up**	**Other ID information collected**
01	*Facebook*	Name, email ID or mobile number (confirmation required), birthday, gender	Profile information, content and other metadata, device and network information including unique identifiers, activity logs, cookie-data, transactional data
02	*WhatsApp*	Mobile number (confirmation required), name, photo (optional)	Profile information, content till delivery (subject to exceptions), address book details, status information, activity log, age, device and network information including unique identifiers and activity information, transactional data

[46] Cookies are small pieces of data stored on a device by an application, that are used to identify a computer or user. They are typically used to customise the browsing experience for individual users. HTTP cookies in fact are built specifically to enable Internet browsers to track, personalise and save information about each browsing session (Anonymous, 2020a). Cookies can be used to easily track a user from website to website, thereby enabling identification of a user and building profiles of individual users (Mayer, 2009).

	Platform	ID information at time of sign-up	Other ID information collected
03	*Gmail*	Name, username, birthday, gender, mobile number (confirmation required), alternate email ID	Profile information, content and related metadata, device and network information including unique identifiers, activity logs, cookie-data, transactional data
04	*TikTok*	Email ID or phone number or existing social media account information (confirmation required), user name, handle, profile description and photo (optional), date of birth	Activity logs, device and network information including unique identifiers, transactional data
05	*Twitter*	Name, email ID or mobile number (confirmation required), date of birth, display name/user name	Profile information, content and related metadata, device and network information including unique identifiers, activity logs, cookie-data, transactional data

Table 1: User ID Information Collected by Major Platforms

Major digital platforms therefore invariably require users to provide some identity information at the time of sign-up (failing which their accounts can be terminated), and also frequently collect identification information during the course of providing services. Importantly, each of the platforms discussed in Table 1 above collects mobile numbers (which are verified in order to gain access to the service), and device and network information, including IP addresses and user activity logs. Thus, while users may be anonymous to other users or indeed at first glance, to the State, the aforementioned major intermediaries will, generally speaking, have the ability to identify them.

Access layer related laws enable identification of users:
Indian law already requires telecom service providers, including internet service providers (collectively TSPs) and cyber cafes to identify users. These intermediaries provide the physical access and network for individuals to connect to platforms and therefore cannot be avoided by users. TSPs must ensure that they "adequately" verify the identity of each subscriber before extending any service to her, in accordance with the format and guidelines laid down by the licensor.[47] This involves filling up a customer acquisition form (CAF), which contains identification details such as a name, address, gender, date of birth, nationality, profession, bank details (for postpaid connections), etc. Identity has to be verified through submission of relevant identification and address proof documents, an Aadhaar number and a picture.[48]

Indeed it is questionable whether such obligations are necessary and proportionate (Bailey, Bhandari & Rahman, 2021; Bailey et al., 2018). While over 155 countries globally are said to require identification

[47] Clause 39.17, Chapter I, UASL.

[48] According to the terms of the Unified Access Service License (UASL), all service providers must preserve their billing and accounting records for a period of three years from the date of publication of audited and approved accounts of the company. Refer Clause 22.3(b), UASL Further, all commercial records, call detail records (CDR), exchange detail records and IP detail records (IPDR) need to be archived for a period of 1 year, unless directed otherwise. Refer Clause 39.20, Chapter VI, UASL. Internet service providers are specifically required to maintain CDR/IPDRs, log-in and log-out details (from services provided by the licensee such as internet access, email, internet telephony, etc.) of all subscribers for a minimum period of 1 year. Refer Clause 7.1, Chapter IX, UASL.

requirements for use of telecom services, countries such as the US, the UK, the Netherlands, and New Zealand do not (Privacy international, 2019).[49]

The discussion above makes it clear that a combination of data sets held by multiple intermediaries at different layers of the Internet can be used by LEAs to identify the real-world identity of users, particularly in view of the ability of LEAs to also access data from TSPs and to carry out relevant reverse-searches, etc. of network data.[50] However, it is pertinent to reiterate the government should not have indiscriminate access to such data as well i.e., the access to this data must be proportionate and subject to appropriate procedural checks, oversight etc. (Bailey et al., 2018).

Thus, a requirement for building in traceability ignores the fact that in today's digital ecosystem, users of online platforms do not necessarily exist in a state of complete or perfect anonymity. It can often be difficult if not impossible for users to actually hide their identities. While indeed privacy concerns have meant that applications such as browsers have begun to collect/store less user data, technological and service provision needs will also imply that some personal data of users will inevitably be collected in the digital ecosystem. Indeed, it is this ability of both the government and the private sector to readily access granular personal data on individuals, which has led to persistent claims of the rise of surveillance societies.

While indeed users may be anonymous to the state or to other users at first glance, the quantity of personal data collected in the digital ecosystem implies that methods of identification are usually available to authorities.[51] Typically, LEAs can approach intermediaries to solicit information on the user - provided either at the time of sign-up or with regard to the data trails that accompany any online activities (Bailey et al., 2018). Indeed, these powers themselves, have been noted to be excessive and without sufficient oversight (Bailey et al., 2018). Even in contexts where say, end to end encryption is used, the metadata associated with the content can generally provide sufficient information to enable traceability of a user in normal cases (Bailey, Bhandari & Rahman, 2021).

We therefore believe that in light of the overwhelming impact of the traceability obligation on the right to privacy, anonymity and free speech of individuals, the questionable impact of identification laws on reducing online offences, the presence of alternative avenues for preventing, investigating and punishing online crimes, as well as the limited nature of safeguards in the law, the traceability provision fails the final prong of the proportionality test.

Calls for traceability and identification of users may therefore be motivated largely by the need to make investigation of offences easier for LEAs. As we have discussed in Bailey, Bhandari and Rahman (2021), democracy requires some inefficiencies in investigative processes as a form of due process safeguard. The absence thereof lowers the costs of carrying out investigations significantly, thereby incentivising fishing or motivated expeditions by law enforcement.

Together with the alternatives available to LEAs as discussed above, the real issue facing law enforcement today may actually relate more to the need to reexamine extant data retention laws and

[49] The absence of a link between identity and phone usage does not take away from the ability of law enforcement to carry out surveillance, though of course it may make matters more difficult. Identity-less phones are equally susceptible to surveillance technologies used by the government through data trails left at the network level, base station logs, etc.

[50] This is of course, subject to the use of masking or other technical methods by which users may hide their identities.

[51] It must also be remembered that the understanding of the term "identification" itself is broad - therefore any method for identification would fall within the scope of 'identifiability' as understood in the PDP Bill.

procedural requirements that govern the manner in which LEAs have access to information required for the investigation and prosecution of offences. Similarly, there are multiple less-intrusive measures that could be adopted at the platform end to enable digital platforms to function in a safer manner. Alternative and non-privacy invasive interventions could for instance, range from implementing easier systems of reporting content to technological nudges, etc.(Bailey & Bhandari, 2021; Bennett & Beverton-Palmer, 2021; Satyavrat, 2021).

4 Conclusion

In this paper, we have critically examined the arguments advanced both for and against anonymity in general and online anonymity in particular, and the different contexts within which anonymity has been safeguarded under Indian law. On the basis of this analysis, we have argued that the right to anonymity should also be recognized as flowing directly from Article 19(1)(a) and Article 21, and safeguarded in the online context, given its varied speech, privacy, and equality benefits. However, we acknowledge that there is merit to user identification online in many cases and this right cannot be absolute. We argue that allowing restrictions of the right to anonymity is a complex exercise and we cannot have a broad brushed approach to unmasking identity of anonymous speakers online. Therefore, the public and individual interests protected by any restriction on the right to online anonymity will have to be examined on a case by case basis and against the proportionality standard. Finally in the paper, we highlight the constitutional concerns that emerge from voluntary verification requirement and the traceability obligation imposed on certain social media intermediaries in the recent Intermediaries Guideline Rules, 2021. We argue that given the overwhelming impact of the traceability obligation on the right to privacy, anonymity and free speech of Internet users in India, the questionable impact of identification laws on reducing online offences, the presence of less intrusive alternatives for preventing, investigating and punishing online crimes, as well as the inadequate nature of safeguards set out in this law, the mandatory traceability obligation imposed on significant social media intermediaries may not pass the proportionality challenge.

References

Agrawal, A. & Pahwa, N. (2019). Why antony clement rubin petitioned madras hc to link aadhaar to social media accounts. Retrieved from https://www.medianama . com / 2019 / 07 / 223 - why - antony - clement - rubin - petitioned - madras-hc-to-link-aadhaar-to-social-media-accounts/

Ahmed, Y. (2021). Whatsapp may soon touch 500 million users in india despite new privacy policy, claims report. Retrieved from https://www.indiatoday.in/technology/news/story/whatsapp-may-soon-touch-500-million-users-inindia- despite-new-privacy-policy-claims-report-1758344-2021-01-12

Aju Varghese v. State of Kerala. (2018). (2018) SCC Online Ker 5397.

Amnesty International. (2020). Shocking scale of abuse on twitter against women politicians in india. Retrieved from https://amnesty.org.in/news-update/shocking-scale-of-abuse-on-twitter-against-women-politicians-in-india/

Anonymous. (2020a). Cookies: What you need to know and how they work. Retrieved from https : / /www. kaspersky. com / resource - center / definitions / cookies

Anonymous. (2020b). Definition of identity. Retrieved from https://www.merriamwebster.com/dictionary/identity

Anonymous. (2021). Case study: South korea's internet identity verification system. Retrieved from https : / / catalystsforcollaboration . org / case - study - internet-identity-verification-system/

Araujo, R. & Gaudiot, A. (2020). Brazil's fake news bill threatens to harm internet freedom and individual rights. Retrieved from https://publixphere.net/i/noc/page/OI_Case_Study_Brazilian_Courts_and_the_Internet.html

Article 29 Data Protection Working Party. (2007). Opinion 4/2007 on the concept of personal data. Retrieved from https : / / ec . europa . eu / justice / article - 29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

Bahl, V., Rahman, F. & Bailey, R. (2020). Internet intermediaries and online harms: Regulatory responses. Retrieved from http://datagovernance.org/report/internet-intermediaries-and-online-harms-regulatory-responses-inindia

Bailey, R. & Bhandari, V. (2021). Towards holistic regulation of online hate speech. IT for Change. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792184

Bailey, R., Bhandari, V. & Goyal, T. (2021). Analysing india's kyc framework through the privacy lens. Forthcoming.

Bailey, R., Bhandari, V., Parsheera, S. & Rahman, F. (2018). Use of personal data by intelligence and law enforcement agencies. Retrieved from https://bit.ly/2CEzCoN

Bailey, R., Bhandari, V. & Rahman, F. (2021). Backdoors in encryption: Analysing an intermediary's duty to provide technical assistance. Retrieved from https://datagovernance.org/report/backdoors-to-encryption-analysing-anintermediarys-duty-to-provide-technical-assistance

Bailey, R., Parsheera, S. & Rahman, F. (2019). Comments on the (draft) information technology (intermediary guidelines (amendment) rules), 2018. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3328401

Bailey, R., Sane, R., Goyal, T. & Varma, R. (2021). Analysing india?s kyc framework: Can we do things better? Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3776008

Barik, S. (2021). Explained: What the challenges to end-to-end encryption in india mean for user rights and national security. Retrieved from https://entrackr.com/2021/06/explained- what- the- challenges- to-whatsapp- end- to- endencryption- in-india/

Bennett, A. & Beverton-Palmer, M. (2021). Social media futures: Anonymity, abuse and identity online. Retrieved from https : / / institute . global /policy /social-media-futures-anonymity-abuse-and-identity-online

Bhandari, V. & Kovacs, A. (2021). What's Sex Got to Do With It: Mapping the Impact of Questions of Gender and Sexuality on the Evolution of the Digital Rights Landscape in India. Retrieved from https://tinyurl.com/y2decf66

Bhandari, V. & Lahiri, K. (2020). The surveillance state: Privacy and criminal investigation in india: Possible futures in a post-puttaswamy world. University of Oxford Human Rights Hub Journal, (2), 15.

Bhandari, V. & Narayan, R. (2018). In striking down section 57, sc has curtailed the function creep and financial future of aadhaar. Retrieved from https : / / thewire . in / law/ in - striking - down- section - 57 - sc - has - curtailed - the - function-creep-and-financial-future-of-aadhaar

Bhandari, V. & Rahman, F. (2020). Constitutionalism during a crisis: The case of aarogya setu app. Retrieved from https://blog.theleapjournal.org/2020/05/ constitutionalism-during-crisis-case-of.html

Bhandari, V. & Sane, R. (2018). Protecting citizens from the state post-puttaswamy: Analysing the privacy implications of the justice srikrishna committee report and the data protection bill, 2018. Socio Legal Review, 143–169.

Bhatia, G. (2014). Free speech and source protection for journalists. Retrieved from https : / / cis - india . org / internet - governance /blog / free - speech- andsource- protection-for-journalists

Blagdon, J. (2012). South korea strikes down law requiring real name use online. Retrieved from https://www.theverge.com/2012/8/24/3264805/southkorea-real-name-law-court-ruling

Boudin, C. (2011). Publius and the petition: Doe v. reed and the history of anonymous speech. Yale Law Journal, 120. Retrieved from https : / /www.yalelawjournal.org/note/publius- and- the- petition- doe- v-reed- and- thehistory-of-anonymous-speech-1

Carville, O., Court, E. & Brown, K. V. (2020). Hospitals tell doctors they'll be fired if they speak out about lack of gear. Retrieved from https ://www.bloomberg.com/news/articles/2020-03-31/hospitals-tell-doctors-they-ll-befired-if-they-talk-to-press

Chandra, A. (2020). Proportionality in india: A bridge to nowhere? University of Oxford Human Rights Hub Journal, (2), 55–86.

Chatterjee, S. (2018). Newsgatherers' privilege to source protection. Retrieved from https://vidhilegalpolicy.in/2018/08/21/2018-8-21-newsgatherers-privilegeto-source-protection/

Cho, D. (2011). Real name verification laws on the internet: A poison or cure for privacy? Retrieved from http://infosecon.net/workshop/downloads/2011/pdf/Real_Name_Verification_Law_on_the_Internet:_a_Poison_or_Cure_for_Privacy.pdf

Citron, D. (2009). Cyber civil rights. B.U. L. REV. 61–64.

Clark, D. D. (1988). The design philosophy of the darpa internet protocols. *Computer Communication Review*, (4), 106–114.

Collins, K. (2015). Why outlawing anonymity will not halt online abuse. Retrieved from https : / /www. wired . co .uk/ article / real - name- policies - anonymityonline- harassment

Daniyal, S. (2015). Internet anonymity in india encourages trolls – but it's also necessary. Retrieved from https://scroll.in/article/734716/internet-anonymityin-india-encourages-trolls-but-its-also-necessary

Dasgupta, P. (2019). Eta ki metoo?': Did indian women find a new language to speak about abuse. Retrieved from https://www.huffingtonpost.in/entry/metoo-india-women-language_in_ 5d94a29ee4b0ac3cddb1913d

Davenport, D. (2002). Anonymity on the internet: Why the price may be too high. Retrieved from https ://www. csl .mtu.edu/cs6461/www/Reading/Davenport02.pdf

Dr. S Krishna Rao v. Ushodaya Publications. (2008). 2008 (2) ALD 819.

Evans, J. (2014). Online anonymity will soon be the only kind we have. Retrieved from https://techcrunch.com/2014/08/30/online-anonymity-will-soon-bethe-only-kind-we-have/

Froomkin, A. M. (2017). Lessons leared too well: Anonymity in a time of surveillance. Arizona LR, 1–63.

Hartzog, W. & Selinger, E. (2015). Surveillance as loss of obscurity. *Washington and Lee Law Review*, (3), 1343–1387.

In re Galavandar v. Unknown. (1957). AIR 1957 Mad 427 (15).

In re: Resident Editor and Ors. Of the Hindustan Times. (1989). Crim. Misc Ptn 7 of 1989, Pat. HC.

Internet Freedom Foundation. (2021). Deep dive : How the intermediaries rules are anti-democratic and unconstitutional. Retrieved from https://internetfreedom.in/intermediaries-rules-2021/

Jai Prakash Agarwal v. Vishambhar Dutt Sharma and Ors. (1986). 1986 DLT 21.

Jain, S. (2018). Make it id of choice for your users. Retrieved from https : / / economictimes.indiatimes.com/blogs/et-commentary/make-it-id-of-choicefor-your-users/

Javed Akhtar v. Lana Publishing Co. (1987). 1987 AIR (Bom) 339.

Jayawardane, M. (2019). Anonymity is a necessary tool for india's metoo movement. Retrieved from https://www.aljazeera.com/indepth/opinion/anonymitytool-india-metoo-movement-191014112350666.html

Justice KS Puttaswamy (Retd.) v. Union of India. (2017). 2017 (10) SCC 1.

Justice KS Puttaswamy (Retd.) v. Union of India. (2019). (2019) 1 SCC 1.

Justice Srikrishna Committee. (2018). A free and fair digital economy: Protecting privacy, empowering indians. Report of the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna. Retrieved from http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

Kang, R., Dabbish, L. & Sutton, K. (2016). Strangers on your phone: Why people use anonymous communication applications. Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work and Social Computing. Retrieved from https://dl.acm.org/doi/10.1145/2818048.2820081

Kaye, D. (2015). Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression. United Nations, Human Rights Council. Retrieved from https ://documents - dds- ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement

Keller, F., Schoch, D., Stier, S. & Yang, J. (2019). It's not easy to spot disinformation on twitter. here's what we learned from 8 political 'astroturfing' campaigns. Retrieved from https : / /www.washingtonpost . com / politics / 2019 / 10 / 28 / its - not - easy - spot - disinformation - twitter - heres - what - we - learned-political-astroturfing-campaigns/

Koops, B.-J. (2010). The internet and its opportunities for cybercrime. Transnational Criminology Manual. Retrieved from https://pure.uvt.nl/portal/en/ publications/the- internet-and- its-opportunities- for-cybercrime(cacedf83- 6d90-404d-b4f8-fa92081234cc).html

Kovacs, A. (2020). When our bodies become data, where does that leave us? Retrieved from https://deepdives.in/when-our-bodies-become-data-wheredoes-that-leave-us-906674f6a969

Langer, L., Jonker, H. & Pieters, W. (2010). Anonymity and verifiability in voting: Understanding (un)linkability. In M. Soriano, S. Qing & J. Lopez (Eds.), Information and communications security (pp. 296–310). Berlin, Heidelberg: Springer Berlin Heidelberg.

Langvardt, K. (2018). Regulating online content moderation. Georgetown L.J. 1353–1388.

Laxmi Singh v. Rekha Singh. (2020). CA arising out of SLP (C) Nos. 10733 - 734 of 2019, Supreme Court of India.

Littleton, T. (2019). Why do people become trolls online? Retrieved from https://thesocialelement.agency /why-people-become-trolls-online

Liu, C. (2014). India's whistleblower protection act — an important step, but not enoughs. Global Anti Corruption Blog. Retrieved from https://globalanticorruptionblog.com / 2014 / 06 / 02 / guest - post - indias - whistleblower - protection - act - an - important-step-but-not-enough/

Lovell v. City of Griffin. (1938). 303 US 444.

Mathi, S. (2021a). All your questions on whatsapp?s end-to-end encryption answered. Retrieved from https ://www.medianama.com/2021/06/223- whatsappencryption-faq/

Mathi, S. (2021b). Whatsapp alleges it rules are unconstitutional in lawsuit against indian government. Retrieved from https : / /www. medianama . com /wpcontent/uploads/2021/05/WhatsApp-v.-Union-of-India-Filing-Version.pdf

Matthan, R. (2019). End-to-end encryption must be retained at all cost. LiveMint. Retrieved from https://www.livemint.com/opinion/online-views/opinionend- to-end-encryption-must-be-retained-at-all-cost-1566926664869.html

Mayer, J. R. (2009). Any person a pamphleteer: Internet anonymity in the age of web 2.0. Retrieved from https://jonathanmayer.org/publications/thesis09.pdf

McCallister, E., Grance, T. & Scarfone, K. (2010). Guide to protecting the confidentiality of personally identifiable information. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/ nistspecialpublication800-122.pdf

Ministry of Electronics and IT. (2021). Press release on whatsapp case. Retrieved from https://internetfreedom.in/intermediaries-rules-2021/

Mitta, M. (2012). No legal cover for journalists refusing to divulge source. Retrieved from https://timesofindia.indiatimes.com/india/No-legal-cover-forjournalists-refusing-to-divulge-source/articleshow/12499518.cms

Mx of Bombay Indian Inhabitant v. Zy. (1997). AIR 1997 Bom 406. NAACP v. Alabama. (1958). 357 U.S. 449.

Nair, R. (2019). Indian twitter is a bastion of masked troll-slayers. Retrieved from https://www.deccan herald.com/metrolife/metrolife-on-the-move/indiantwitter-is-a-bastion-of-masked-troll-slayers-751967.html

Naresh Shridhar Mirajkar v. State of Maharashtra. (1966). 1966 SCR (3) 744.

Nipun Saxena v. Union of India and Ors. (2019). (2019) 2 SCC 703.

Oster, J. (2015). Cambridge University Press.

Parsheera, S. & Bailey, R. (2018). The aadhaar judgement uses the right-to-privacy test in two completely different ways. Retrieved from https://tinyurl.com/y328ahhv

Patient X v Hospital Z. (1998). 1998 Supp (1) SCR 723.

Patrick Breyer v. Bundesrepublik Deutschland. (2016). C-582/14, European Court of Justice.

Prabhakaran, M. (2019). On a proposal for originator tracing in whatsapp. Retrieved from https : / / internetfreedom . in / iff - files - independent - expert - submission-before-madras-hc/

Prasanna. (n.d.). Section 57: Why aadhaar can't be used as authentication by private companies. Retrieved from https://www.medianama.com/2018/09/223- section-57-why-aadhaar-cant-be-used- as-authentication-by- privatecompanies/

Privacy international. (2019). Timeline of sim card registration laws. Retrieved from https://privacyinternational.org/long-read/3018/timeline-sim-cardregistration-laws

PTI. (2015). Journalist burnt to death; up minister booked. Retrieved from https://www.thehindu.com /news/national/other-states/up-minister-booked-injournalist-killing-case/article7298669.ece

Rainie, L., Anderson, J. & Albright, J. (2017). The future of free speech, trolls, anonymity and fake news online. PEW Research Centre. Retrieved from https://www.pewresearch.org/internet/2017/03/29/the-future- of- freespeech-trolls-anonymity-and-fake-news-online/

Reddy, P. (2018). Back to the drawing board: What should be the new direction of the intermediary liability law? NLUD Journal of Legal Studies, 1. Retrieved from https://bit.ly/2qZtPZi

Rekha Singh v. State of Uttar Pradesh. (2019). W.P. (C) No. 36490/2018, All. HC.

Rigby, K. (1995). Anonymity on the internet must be protected. Retrieved from http://groups.csail.mit.edu /mac/classes/6.805/student- papers/fall95-papers/rigby-anonymity.html

Sang-Hun, C. (2012). South korea court rejects online name verification law. Retrieved from https://www.nytimes.com/2012/08/24/world/asia/southkorean-court-overturns-online-name-verification-law.html

Satyavrat, K. (2021). The wages of fear: A compendium of global and domestic encryption debates. Retrieved from https://hasgeek.com/PrivacyMode/it-rules- il- guidelines-2021/sub/the-wages- of- fear-a-compendium- of- globaland-domes-GzdvpEhXmLH6uyMaNT2gJx

Scheiber, N. & Rosenthal, B. (2020). Nurses and doctors speaking out on safety now risk their job. Retrieved from https://www.nytimes.com/2020/04/09/business/coronavirus-health-workers-speak-out.html

Sebastian, J. & Sen, A. (2020). Unravelling the role of autonomy and consent in privacy. *Indian Journal of Constitutional Law*, 1–37.

Seth, S. (2010). Protected by online anonymity, hate speech becomes an online mainstay. CNN. Retrieved from https://edition.cnn.com/2010/LIVING/08/16/online.anonymity/index.html

Shao, G. (2019). Social media has become a battleground in hong kong's protests. Retrieved from https ://www.cnbc .com/2019/08/16/social - media- hasbecome- a-battleground-in-hong-kongs-protests.html

Sharma, Y. & Qadir, G. (2020). ''people are vanishing'': In kashmir, twitter users remove digital footprints as police cracks whip. Retrieved from https : / / thekashmirwalla.com/2020/08/people- are- vanishing- in-kashmir- twitterusers- remove-digital-footprints-as-police-cracks-whip/

Silva, I. & e Fernanda Cohen, D. L. (2017). Sarahah and secret: Notes on apparent anonymity in internet applications. Retrieved from https://www.lickslegal.com/articles/sarahah-and-secret-notes-on-apparent-anonymity-in-internetapplications

Sircar, S. & Sachdev, V. (2020). 'riteish deshmukh?, lord hanuman and pak spy get pm kisan cash as farmers. Retrieved from https://www.thequint.com/cyber/pm-kisan-scam-aadhaar-riteish-deshmukh-hanuman-pakistan-spyget-cash-as-farmers#read-more

Skopek, J. (2015). Reasonable expectations of anonymity. *Virginia Law Review*,691–762.

Smith, T. (2019). In hong kong, protestors fight to stay anonymous. Retrieved from https://www.theverge .com/2019/10/22/20926585/hong-kong-chinaprotest-mask-umbrella-anonymous-surveillance

Solove, D. (2006). A tale of two bloggers: Free speech and privacy in the blogosphere. *Washington University Law Review,* (5), 1195–1200.

Somanchi, A. (2018). Aadhaar fraud is not only real, but is worth more closely examining. Retrieved from https://thewire.in/economy/aadhaar-fraud-uidai

Souza, C. A. & Lemos, R. (n.d.). Brazilian courts and the internet ? rulings before and after the marco civil on intermediary liability. Retrieved from https ://publixphere.net/i/noc/page/OI_Case_Study_Brazilian _Courts_and_the_Internet.html

Stein, E. (2003). Queers anonymous:lesbians, gay men, free speech, and cyberspace. *Harv. Civil Rights-Civil Liberties L.R. 38.*

Stoeffel, K. (2014). Women pay the price for the internet's culture of anonymity. Retrieved from https://www.thecut.com/2014/08/women-pay-the-pricefor-online-anonymity.html

Subodh Gupta v. Herdscene and Ors. (2019). CS (OS) 483/2019, Del. HC.

Suchindran, B. & Pandya, P. (2018). Are electoral bonds an elaborate ruse to protect anonymous donations? Retrieved from https://economictimes.indiatimes.com/blogs/et-commentary/is-electoral-bonds-scheme-an-elaborate-ruse-toprotect-anonymous-donations/

Suler, J. (2004). The online disinhibition effect. *CyberPsychology and Behaviour*,7, 321.

Surakha P. (2017). Less than 50 percent hiv patients link aadhaar to anti-retroviral therapy services. Retrieved from https : / / www . newindianexpress . com / states/karnataka/2017/oct/30/less - than- 50-percent - hiv- patients - link - aadhaar-to-anti-retroviral-therapy-services-1686682.html

Thapliyal, N. (2021). Traceability rule will break end-to-end encryption; can put privacy of journalists, activists, politicians at risk : Whatsapp tells delhi high court. Retrieved from https://www.livelaw.in/news-updates/whatsappdelhi-high-court-traceability-end-to-end-encryption-privacy-risk-174743?infinitescroll=1

Twitter Help. (2021). About verified accounts. Retrieved from https ://bit . ly/34RcWQA

Upadhyay, J. (2019). Just how safe are whistleblowers under indian law? LiveMint. Retrieved from https://www.livemint.com/news/india/just-how-safe-arewhistleblowers-under-indian-law-11571763505941.html

Vaishnav, M. (2019). Electoral bonds: The safeguards of indian democracy are crumbling. Retrieved from https://carnegieendowment.org/2019/11/25/electoral-bonds-safeguards-of-indian-democracy-are-crumbling-pub-80428

Wang, S. A., Pang, M.-S. & Pavlou, P. A. (2014). Virtues and perils of anonymity: Should intermediaries bear the burden? Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3249479

Web Desk. (2019). Explained: The legal challenge to whatsapps encryption in india. Retrieved from https://www.theweek.in/news/biz-tech/2019/08/15/explained-the-legal-challenge-to-whatsapps-encryption-in-india.html

Xinhua News Agency. (2017). The network real-name system is fully coming, how to ensure that our virtual space is more “fresh”. Retrieved from http://www.xinhuanet.com/live/2017-08/30/c_136568575.htm

Zingales, N. (2018). ’cure or poison?’ identity verification and the spread of fake news on social media. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2463564

Acknowledgements

We thank participants at the Data Governance Network meetings of August 6 and October 28, 2020, Smriti Parsheera, Gaurav Jain, Udbhav Tiwari, Divij Joshi and Devendra Damle for comments and discussions. All errors are our own.

About the Authors

Rishab Bailey is a lawyer and technology policy researcher at the National Institute of Public Finance and Policy, New Delhi. Vrinda Bhandari is an advocate at the Delhi High Court. She is involved in challenging the Intermediary Liability Rules, 2021, before the Kerala High Court. Faiza Rahman is a PhD candidate at the University of Melbourne, Australia. Authors are listed in alphabetical order. All errors are our own

datagovernance.org dgn@idfcinstitute.org

@datagovnetwork /datagovnetwork /datagovnetwork