"The Online Intermediary Research Project"

Commissioned by:
University of Washington (UW) – Google

on

Online Intermediary Liability and Privacy in India

Yogesh Pai and Nitesh Daryanani

Abstract

Online intermediaries are entities that facilitate all of the transactions that take place on the internet. The extent of the data that flows through such intermediaries on a daily basis presents several privacy concerns, which are the subject of this Report. In India, the right to privacy is not explicitly guaranteed by the Constitution, but the Supreme Court has interpreted Article 21 of the Constitution (which provides for the right to life or personal liberty) as implicitly granting the right to privacy. In furtherance of the mandate to secure the right to privacy of individuals in India, the Government has introduced a host of legislative measures that seek to (i) protect the data collected by intermediaries from individuals, and (ii) protect individuals from infringement of their right to privacy via content that is hosted by intermediaries. Currently, these laws are fragmented and are largely sector-specific. In the context of the internet, the Information Technology Act 2000 requires intermediaries to protect the data they collect and handle, and imposes conditional liability on intermediaries for their hosted content if such content infringes the privacy of an individual. However, these laws are inadequate to deal with the new concerns that have arisen as a result of the rapid advances in technology and re-shaping of the internet. Keeping in mind these concerns, a Group of Experts on Privacy was convened in order to analyze the state of India's law on privacy and make recommendations that would form the basis for a new privacy framework in India. These recommendations have resulted in a draft Privacy Bill, which takes significant steps toward harmonizing the data protection standards and intermediary liability laws in India with those of the rest of the world.

About the Authors

Yogesh Pai is currently an Assistant Professor at National Law University, Delhi. He teaches and writes in the area of intellectual property law and policy and researches issues regarding the interface of technology, economics, and policy. He has previously worked with the South Centre in Geneva, Centad, New Delhi, and was the MHRD IPR Chair Coordinator at National Law University, Jodhpur – India. Yogesh serves as the legal member of an ad hoc committee constituted by the Government of India to assess the granting of compulsory licences for affordable healthcare in India. Previously, he was part of an ad hoc expert committee formed to examine the need for utility models in India. Yogesh is also interested in reforms in Indian legal education. His publications are available at: https://nludelhi.academia.edu/YogeshPai.

Nitesh Daryanani is a graduate of National Law University, Jodhpur, having completed his B.B.A., LL.B. (Intellectual Property Law Honours) in 2012. Currently, he is working as Research Fellow at the Centre for Innovation, Intellectual Property, and Competition, at National Law University, Delhi. From 2012 to 2016, he had been working in the chambers of Mr. Neeraj Kishan Kaul, the Additional Solicitor General of India in the Supreme Court. In 2014, he was engaged as Panel Counsel for conducting the Central Government's litigation before the Supreme Court of India. During his four years in practice, he has dealt with a wide variety of litigation, on subjects including constitutional law, intellectual property law, competition law, and taxation law.

Introduction

Within the structure of the internet, intermediaries act as the channels through which the network functions. The definition of an intermediary, as espoused by the Organization for Economic Co-operation and Development (OECD), is an entity that "brings together or facilitates transactions between third parties and the internet. They give access to, host, transmit and index content, products and services originated by third parties on the internet to provide internet-based services to third parties."[1]

Broadly speaking, intermediaries are the entities that facilitate a user's access to content on the internet – by either acting as a platform to host content or as a conduit to facilitate transmission. They provide a means for online exchange without obtaining title over the exchanged items or information; rather, transactions or exchanges take place between third parties via the intermediaries' platforms.[2] It is widely recognized that these intermediaries are essential cogs in the wheel of the internet.[3]

In India, an intermediary is broadly defined in Section 2(1)(w) of the Information Technology Act 2000 as any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record; this includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes.[4] Therefore, if an entity serves as a platform for the exchange of information, goods, or services via the internet, such an entity would satisfy the definition of an "intermediary" under Section 2(1)(w) of the Information Technology Act 2000. Such an entity would "receive, store or transmit" data on behalf of its users, and in some cases, even provide services in relation to this data, and therefore would fall within the broad scope of Section 2(1)(w).

---

[1] OECD, *The Economic and Social Role of Internet Intermediaries* (Apr. 2010), https://www.oecd.org/internet/ieconomy/44949023.pdf.

[2] Copenhagen Economics, *Closing the Gap – Indian Online Intermediaries and a Liability System Not Yet Fit for Purpose* (Mar. 2014), https://www.globalnetworkinitiative.org/sites/default/files/Closing%20the%20Gap%20-%20Copenhagen%20Economics_March%202014_0.pdf.

[3] Rishabh Dara, *Intermediary Liability in India: Chilling Effects on Free Expression on the Internet*, Centre for Internet & Society – Bangalore (Apr. 10, 2012), http://cis-india.org/internet-governance/intermediary-liability-in-india.

[4] Information Technology (Amendment) Act 2008, No. 10, Acts of Parliament, 2009 (India), Section 2(1)(w): ((w): "intermediary" with respect to any particular electronic message, means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message).

In the 1990s, when the internet was still coming into its own, intermediaries were subject to only limited regulation.[5] In recent years, they have grown to provide a thriving platform through which information exchange takes place on a grand scale every day. India is at the centre of this revolution, both in terms of providing internet-related services as well as "consuming" the internet. While India has grown into one of the leading IT service providers to businesses across the globe, its own internet user base stood at 306 million users at the end of 2015 and is expected to reach 371 million users by June 2016, per a Report by the Internet and Mobile Association of India (IAMAI).[6]

The scale on which information is transmitted across borders has also facilitated the commission of various unlawful acts, such as defamation, invasion of privacy, and intellectual property infringement.[7] The chief cause of this increase in unlawful activity is the increasing amount of data flowing to and being held by intermediaries providing services on the internet. For instance, transmission of data over the internet is fraught with the risk of interception, and stored information is susceptible to security breaches.[8] These risks raise concerns due to the potential harm they can inflict upon the privacy of an individual. In this setting, it becomes necessary to both clearly conceptualize the privacy right of an individual and to regulate the manner in which an individual's information is collected and used by online intermediaries, so as to ensure that this right to privacy is not harmed.

This Report seeks to achieve this purpose. First, it will trace the evolution of the right to privacy, and apply it to the context of an individual's transactions on the internet. Next, the Report will comprehensively document the extent to which the right to privacy is recognized in India, based primarily on the Supreme Court's jurisprudence. Thereafter, it will analyse the obligations imposed on intermediaries in India in order to safeguard the right to privacy.

For this purpose, the authors find that the best approach is to divide intermediaries' activities into two categories, based on whether such activity gives rise to primary or secondary liability. In cases where an individual has provided "information" to an intermediary and such information is deliberately or unknowingly disclosed by the intermediary, there may be a direct infringement of the injured user's privacy. On the other hand, if an intermediary's service is used by a third party to commit an act

---

[5] Article 19 Free Word Centre, *Internet Intermediaries: Dilemma of Liability* (2013),https://www.article19.org/data/files/Intermediaries_ENGLISH.pdf.

[6] PTI, *Mobile Internet users in India to reach 371 mn by June 2016*, INDIAN EXPRESS (Feb. 4, 2016),http://indianexpress.com/article/technology/tech-news-technology/mobile-internet-users-in-india-to-reach-371-mn-by-june-2016/.

[7] Pritika Rai Advani, *Intermediary Liability in India*, ECONOMIC & POLITICAL WEEKLY VOL. 48, ISSUE NO. 50 (Dec. 14, 2013), http://www.epw.in/author/pritika-rai-advani.

[8] Prashant Iyengar, *Privacy and the Information Technology Act in India* (Apr.5, 2011), http://ssrn.com/abstract=1807575.

which infringes the privacy right (or any other right) of an individual, and the intermediary fails to demonstrate that it has exercised a reasonable standard of care in monitoring the content hosted by it, it may be found secondarily liable for the infringement. Depending on the nature of the concern, the right to privacy of individuals can be secured by three means: (a) self-regulation, or the governance of the internet by the participants themselves, without intervention by the State; (b) privacy-enabling technology architecture; or (c) through state action, in the form of laws.[9] For the purpose of this Report, its analysis will be restricted to the regulation of intermediaries in India through the operation of law.

The Concept of Privacy

The roots of the concept of privacy may be traced as far back as the teachings of Aristotle in ancient Greece, in the distinction he drew between politics (*polis*) and the domestic space (*oikos*).[10] Over time, this concept has evolved into two distinct legal forms: (i) as an action for damages under tort law, as in cases where one's privacy has been unlawfully invaded; and (ii) constitutional recognition of individuals' right to privacy against unlawful Government intrusion.

Under tort law, the seminal formulation of privacy by William Prosser was based on the nature of the conduct and injury caused in each case (e.g., unreasonable intrusion into the individual's seclusion, appropriation of name or likeness, bringing unreasonable publicity to the individual's personal life, and publicity in false light).[11] This approach is intricately linked to the liberty-driven conception of privacy held in the United States, summed up by Charles Warren and Louis D. Brandeis as an individual's "right to be let alone," that he must be able to assert directly.[12] This view has been adopted in the constitutional jurisprudence on privacy in India, as in *Gobind v. State of Madhya Pradesh* the Supreme Court stated that "individuals need a place of sanctuary where they can be free from societal control. The importance of such a sanctuary is that individuals can drop the mask, desist for a while from projecting on the world the image they want to be accepted as themselves, an image that may reflect the values of their peers rather than the realities of their natures."[13]

However, this liberty-centric approach is insufficient to address the myriad privacy concerns that have arisen in the digital age. The internet is unique in the sense that it solicits information from users every step of the way, as a necessary precondition for participation in cyberspace. By disclosing data to intermediaries on the internet, the

---

[9] Ujwala Uppaluri and Varsha Shivanagowda, *Preserving Constitutive Values in the Modern Panopticon: The Case for Legislating Toward a Privacy Right in India*, 5 NUJS L. REV. 21 (2015).
[10] *Id.*
[11] William L. Prosser, *Privacy*, 48 CAL. L. REV.383 (1960).
[12] Samuel Warren and LouisBrandeis, *The Right to Privacy*, 4 HARVARD L. REV. 193 (1890).
[13] *Gobind v. State of Madhya Pradesh*, (1975) 2 SCC 148 (India).

individual is in a sense putting his or her information in the public domain. Indeed, this concern was nicely captured by Judge Posner, when he stated that "the fact that one cannot negotiate modernity without continuously revealing personal information to a variety of demanders has habituated most … to radically diminished informational privacy."[14] In this context, a more relevant way to construe the right to privacy is as a concept intricately linked to the dignity of an individual; this is in line with the view held in the European Union.[15]

Daniel Solove recognized that Prosser's conception of privacy was inadequate to address the concerns that arise in the context of the internet. He stated that any attempt to apply these conceptions of privacy torts to potential harms on the internet may fall afoul of the "third party doctrine," which dictates that the right to privacy cannot be infringed once the data at issue is in the public domain. Solove instead proposed a new taxonomy of privacy harms that would focus on the nature of the activities causing such harm – information collection, information processing, information dissemination, and invasion.[16] While the nature of activities and the corresponding harm caused are different areas of focus, there is a common thread that can form the basis for defining the right to privacy (e.g., as the claim of individuals to determine for themselves when, how, and to what extent information about them is communicated to others).[17]

The right to privacy is now recognized internationally as a basic human right, and several international treaties and agreements create an obligation to protect the privacy of individuals. One such instrument, the Universal Declaration of Human Rights (UDHR),[18] was adopted by the United Nations (UN) in 1948, and represents the first comprehensive agreement between nations on the specific rights and freedoms of all human beings. India voted in favour of Article 12 of the UDHR, which provides for the right to privacy in stating that an individual would have the right to protection of the law against any arbitrary interference.

In 1979, India ratified the International Covenant on Civil and Political Rights (ICCPR). Article 17 of the ICCPR states that "[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, correspondence, nor to unlawful attacks on his honor and reputation," and that "[e]veryone has the right to protection of the law against such interference or attacks."[19] However, India has not signed the First Optional Protocol to the ICCPR, and therefore it is not possible for

---

[14] Richard A. Posner, *Privacy, Surveillance, and Law*, 75 UNIV. OF CHICAGO L. REV. 245 (2008).
[15] Uppaluri and Shivanagowda, *Preserving Constitutive Values*, *supra* note 9.
[16] Daniel J. Solove, *A Taxonomy of Privacy*, 154 UNIV. OF PENNSYLVANIA L. REV. 477 (2006).
[17] Uppaluri and Shivanagowda, *Preserving Constitutive Values*, *supra* note 9.
[18] G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948).
[19] This language is similar to Article 8(1) of the European Convention on Human Rights 1950, which provides that "everyone has the right to respect for his private and family life, his home, and his correspondence."

Indian citizens to make a complaint or "communication" to the UN based on a failure by India to fully implement Article 17 of the ICCPR.[20]

The Right to Privacy in India

In the Indian domestic context, the right to privacy is not specifically provided for or defined in the Constitution of India. Rather, the right has been read into and built on the foundation of Article 21 of the Constitution of India 1950, which provides that "no person shall be deprived of his life or personal liberty except according to a procedure established by law." Although the National Commission to Review the Working of the Constitution proposed an amendment to the Constitution that would grant an explicit right to privacy,[21] such an amendment never became a reality.[22]

Amongst its earliest Article 21 jurisprudence, the Supreme Court was called upon to determine whether certain Regulations that granted the police wide discretion to carry out surveillance infringed individuals' constitutional right to life and personal liberty. Two such measures were the powers to (i) to carry out periodical inquiries and reporting of movements of a suspect from his home, and (ii) to carry out domiciliary visits at night.[23] The Supreme Court observed that Article 21is based on the Fifth and Fourteenth Amendments to the U.S. Constitution, which read "[n]o person … shall be deprived of life, liberty or property without due process of law," but noted that the scope of protection granted by Article 21 may be narrower than that guaranteed by its United States counterparts, because the word "liberty" was qualified by using the word "personal." Nevertheless, the Court refused to adopt an excessively narrow interpretation of the right to privacy under Article 21, and came to the conclusion that "personal liberty" is a compendious term which includes all the varieties of rights which make up the "personal liberties" of man other than the "freedom" guaranteed under Article 19(1) of the Constitution. In other words, Article 19(1) of the Constitution deals with particular species or attributes of freedom, whereas Article 21 covers residual rights that serve to more fully ensure the "freedom" of citizens.

The Supreme Court opined that the term "personal liberty" must be construed in light of the goal of furthering the dignity of the individual, a phrase that is found in the Preamble to the Constitution of India. Therefore, even though the Constitution of India does not contain language akin to the Fourth Amendment of the U.S.

---

[20] Graham Greenleaf, *Promises and Illusions of Data Protection in Indian Law*, 1.1 INTERNATIONAL DATA PRIVACY LAW 47 (Mar. 2011).

[21] Advisory Panel on Enlargement of Fundamental Rights, *A Consultation Paper on Enlargement of Fundamental Rights*, NATIONAL COMMISSION TO REVIEW THE WORKING OF THE CONSTITUTION (May 11, 2001), http://lawmin.nic.in/ncrwc/finalreport/v2b1-3.htm.

[22] Uppaluri and Shivanagowda, *Preserving Constitutive Values*, *supra* note 9.

[23] *Kharak Singh v. State of Uttar Pradesh*, (1964) 1 SCR 332.

Constitution,[24] the Supreme Court relied on the English common law maxim that "every man's house is his castle," and unanimously held that the unauthorised intrusion into a man's home by police, and the disturbance caused to him thereby, is a violation of his right of personal liberty as protected under Article 21 of the Constitution.

However, the majority held that the power to carry out periodical inquiries and reporting of movements of a suspect from his home did not infringe any fundamental individual rights, since "the right of privacy is not a guaranteed right under our Constitution and therefore the attempt to ascertain the movements of an individual which is merely a manner in which privacy is invaded is not an infringement of a fundamental right." In a seminal opinion exhibiting significant foresight, J. Subba Rao authored the minority view, addressing the question as to whether a citizen has the right to lead a life free from being subject to social control, even if that control was imposed by a valid law. His opinion held that the right of personal liberty in Article 21 was comprehensive enough to include privacy as well, which is the right to be free from restrictions or encroachments upon one's private life, whether such limits are directly imposed via calculated measures or are inadvertently brought about.

A decade later, similar Regulations vesting the police with surveillance powers were challenged before the Supreme Court as violating the fundamental rights guaranteed under Article 19(1)(d) and Article 21 of the Constitution of India [25] Drawing inspiration from J. Subba Rao's dissenting opinion in *Kharak Singh*, the Supreme Court held that the right to privacy encompassed and protected the personal intimacies of the home, family, marriage, motherhood, procreation, and child rearing. This holding was based on the conclusion that the rights and freedoms of citizens set forth in the Constitution guarantee that the individual, his personality, and the things stamped with his personality shall be free from official interference except where a reasonable basis for intrusion exists. Recognizing that it is difficult to arrive at a conclusive definition of the essence and scope of the right to privacy, the Court held that it may include any allied right which is "implicit in the concept of ordered liberty."

However, the Supreme Court also held that the right to privacy must be viewed in the context of other rights and values, and also that the right to privacy maybe denied if a countervailing State interest of paramount importance can be demonstrated. Consequently, the Court held that the right to privacy is not an absolute right, and the scope of the right would have to be determined on a case-by-case basis. Eventually,

---

[24] U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated; and no warrants shall issue but upon probably cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized").

[25] *Gobind v. State of Madhya Pradesh,* (1975) 2 SCC 148.

the Supreme Court upheld the Regulations after holding that they served a compelling State interest and were not unreasonable restrictions on the right to privacy, as long as surveillance was restricted to cases where reasonable evidence exist to induce the opinion that the suspect shows "a determination to lead a life of crime."

It was to be two more decades before the Supreme Court was presented with an opportunity to further chisel the contours of the right to privacy, in a case where individuals' privacy was pitted against the freedom of the press.[26] While reaffirming the view that the right to privacy is implicit in the right to life and liberty guaranteed by Article 21, the Court held that a third party who published material based on information that fell within the scope of another individual's right to privacy would be liable in an action for damages. However, in balancing the right to privacy with the freedom of the press, the Supreme Court held that the right to privacy did not apply once a matter became a part of the public record, and it instead became a legitimate subject for comment by the press and media, among others.

In *People's Union for Civil Liberties (PUCL) v. Union of India & Anr.*,[27] the Supreme Court was faced with a challenge to the constitutionality of Section 5(2) of the Indian Telegraph Act 1885,[28] which vests the Government with the power to carry out telephone-tapping of any person or class of persons in the interest of public safety or in the event of a public emergency. In the alternative, it was argued that the provision should be read to include procedural safeguards to rule out arbitrariness and to prevent indiscriminate telephone-tapping.

From the outset, the Court recognized that the right to hold a telephone conversation in the privacy of one's home or office without interference can be claimed as within the "right to privacy," and held that telephone-tapping would infringe Article 21 of

---

[26] *R. Rajagopal v. State of Tamil Nadu & Ors.*, (1994) 6 SCC 632.

[27] *People's Union for Civil Liberties (PUCL) v. Union of India & Anr.*, (1997) 1 SCC 301.

[28] Indian Telegraph Act, 1885, No. 13, Acts of Parliament, 1885 (India), Section 5 (Power for Government to take possession of licensed telegraphs and to order interception of messages

> (2) On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorised in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order:
>
> > Provided that the press messages intended to be published in India of correspondents accredited to the Central Government or a State Government shall not be intercepted or detained, unless their transmission has been prohibited under this sub-section.).

the Constitution unless it was permitted under a procedure established by law. The Supreme Court's articulation of the right to privacy in this regard was as follows:

> "The right to privacy – by itself – has not been identified under the Constitution. As a concept it may be too broad and moralistic to define it judicially. Whether right to privacy can be claimed or has been infringed in a given case would depend on the facts of the said case. But the right to hold a telephone conversation in the privacy of one's home or office without interference can certainly be claimed as "right to privacy." Conversations on the telephone are often of an intimate and confidential character. Telephone conversation is a part of modern man's life. It is considered so important that more and more people are carrying mobile telephone instruments in their pockets. Telephone conversation is an important facet of a man's private life. Right to privacy would certainly include telephone conversation in the privacy of one's home or office. Telephone-tapping would, thus, infract Article 21 of the Constitution of India unless it is permitted under the procedure established by law."

While noting that Section 5(2) of the Indian Telegraph Act 1885 provides the substantive basis for exercising such telephone-tapping power by laying down the situations and conditions under which it can be exercised, the Court cautioned that the power must also be exercised pursuant to established procedures to ensure that its use is fair and reasonable. Despite the fact that the Telegraph Act had been in effect for more than a century, the Government had failed to make rules regulating the exercise of the powers provided under Section 5(2). Therefore, the Supreme Court laid down guidelines that would govern the Government's invocation of its power to carry out telephone-tapping, such as the requirement to maintain records, a two-month limitation on the duration of such telephone-tapping, and putting an oversight mechanism in place.

In *Mr. X v. Hospital Z,*[29] the Supreme Court held that the disclosure of Mr. X's having AIDS by his doctor to Mr. X's fiancée, which led to their marriage being called off, was not a violation of Mr. X's right to privacy. The Court recognized that public disclosure of true but private facts may amount to an invasion of the right to privacy, since "disclosure of even true private facts has the tendency to disturb a person's tranquillity. It may generate many complexes in him and may even lead to psychological problems. He may, thereafter, have a disturbed life all through."

However, the case presented the Court with a tension between fundamental rights: a person's right to privacy or "right to be let alone" on the one hand, and another's right

[29] *Mr. X v. Hospital Z,* (1998) 8 SCC 296.

to life and health on the other. The Court held that such a conflict must be resolved by enforcing the right that would best advance the public morality or public interest in the specific case. Crucially, the Court noted that "moral considerations cannot be kept at bay and the Judges are not expected to sit as mute structures of clay in the hall known as the courtroom, but have to be sensitive, 'in the sense that they must keep their fingers firmly upon the pulse of the accepted morality of the day.'" This judgment is noteworthy due to its examination of the impact of the right to privacy between private parties, in contrast to the cases involving Government infringement discussed previously. However, the Court did not significantly analyse the enforceability of the right to privacy in such a private context, having held that the right to privacy must give way to another's right to life.

In *District Registrar v. Canara Bank*,[30] the Supreme Court upheld a customer's right to privacy in records stored by a financial institution, such as a bank. In doing so, the Court struck down Section 73 of the Indian Stamp Act 1899 as unconstitutional. Section 73 vested a Government authority with the power to conduct an inspection of any records, registers, books, or documents currently in the custody of a public office, and stated that such investigation required only a belief that it would prove or lead to the discovery of fraud or omission in relation to any duty. Pertinently, the Supreme Court observed that the concept of privacy relates to a citizen rather than a place; therefore, it does not matter whether the financial records were stored in a citizen's home or in a bank. This judgment recognized that the value of information pertaining to a particular individual did not vary based on its location, and brought such information within the ambit of protection afforded by the right to privacy.

Therefore, an analysis of the law laid down by the Supreme Court establishing the contours of an individual's right to privacy reveals that individuals have the right to be free from restrictions or encroachments in their private lives, which include their personalities and things stamped with their personalities. However, this right is subject to reasonable restrictions that are justified by countervailing interests of the State or public. The scope of the right to privacy in India is largely in line with the protections guaranteed in the United States[31] and the European Union,[32] even though India has drawn equally from the liberty-inspired approach in the United States and the dignity-centric approach used by the European Union.

However, the scope of the right to privacy in India was at issue before the Supreme Court in 2015,[33] when the Government sought to implement the "Aadhaar Card Scheme," which would include the issuing of a "multi-purpose national identity card"

---

[30] *District Registrar v. Canara Bank*,(2005) 1 SCC 496.
[31] U.S. CONST., amend. XIV.
[32] European Convention of Human Rights, art. 8, Sept. 3, 1953, C.E.T.S. No. 5.
[33] *K.S. Puttaswamy (Retired) & Anr. v. Union of India & Ors.*, (2015) 8 SCC 735.

to every citizen.[34] This system would operate by collecting demographic and biometric data from individuals that would be used for a number of purposes, including facilitating a Public Distribution System. It was argued that the collection of such data was a violation of individuals' right to privacy, and the legislation establishing this system has been severely criticized for lacking any procedures for establishing proper safeguards.[35]

The Attorney General, appearing for the Government, argued that the very status of the right to privacy as a fundamental right is in doubt, relying on the Supreme Court's observations in *Kharak Singh*.[36] Even though subsequent judgments have clearly stated that the right to privacy is a fundamental right implicit in Article 21 of the Constitution, they were delivered by benches of lesser strength than that which delivered the judgment in *Kharak Singh*, and may be *per incuriam.* Accepting this argument, the Supreme Court referred the matter to a larger bench of appropriate strength in order to clarify the issue. Nevertheless, in view of the evolution of the right to privacy by the Supreme Court in the judgments discussed above, it appears unlikely that the Supreme Court will ultimately hold that the right to privacy is not a fundamental right implicitly guaranteed under the Constitution of India.

The conclusion that emerges from the analysis of these judgments is that the right to privacy of an individual has been protected against State action, but thus far has not been extended to the context of infringement by another private person. The consistent thread through these judgments is the Supreme Court's refusal to define the right to privacy in categorical terms, instead allowing it to evolve on a case-by-case basis. Therefore, it is entirely plausible that the right to privacy implied by Article 21 of the Constitution of India may come to be interpreted as imposing a positive obligation on the State to ensure effective protection of its citizens' right to privacy. This was the interpretation adopted by the European Court of Human Rights[37] in the

---

[34] Kalyani Menon Sen, *Aadhar: Wrong Number, or Big Brother Calling?*, 11.2 SOCIO-LEGAL REV.85 (2015), http://www.sociolegalreview.com/wp-content/uploads/2015/12/Aadhaar-Wrong-Number-or-Big-Brother-Calling.pdf.

[35] Chinmayi Arun, *Privacy is a fundamental right*, THE HINDU (Mar.18, 2016), http://www.thehindu.com/opinion/lead/lead-article-on-aadhaar-bill-by-chinmayi-arun-privacy-is-a-fundamental-right/article8366413.ece.

[36] *Kharak Singh v. State of Uttar Pradesh*, (1964) 1 SCR 332.

[37] *Craxi (No. 2) v. Italy*, (Oct. 17 2003), Application No. 25337/94.

> (73. Nevertheless, the Court recalls that while the essential object of Article 8 is to protect the individual against arbitrary interferences by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this negative undertaking, there may be positive obligations inherent in effective respect for private life … The Court therefore needs to ascertain whether the national authorities took the necessary steps to ensure effective protection of the applicant's right to respect for his private life and correspondence.
>
> 74. In this context, the Court considers that appropriate safeguards should be available to prevent any such disclosure of a private nature as may be inconsistent

context of Article 8 of the European Convention on Human Rights, when it held that failure to prevent leaks of telephone transcripts to the press constituted a failure of the State to fulfil its obligation to secure the applicant's right to respect for his private life and correspondence.

Nevertheless, while it is unclear whether there is a positive obligation upon the State to protect an individual's right to privacy, the need to regulate this right between individuals *inter se*[38] forms the basis of the State's efforts towards putting in place a legal framework: the existing Information Technology Act 2000 and the proposed Privacy Bill 2014.

In the next two sections, this Report examines the means by which individuals' right to privacy has been secured with respect to their activities on the internet, framed by the concepts of primary and secondary liability.

Primary Liability

In the digital era, data has acquired immense significance as the currency with which the internet's economy trades. Data has a multiplicity of uses and attached value, which is apparent from the fact that most popular social media services, such as Twitter and Facebook, do not charge users for their services and instead generate significant revenue through the sale of user demographic information to advertisers. This "information market" presents significant potential to harm an individual's right to privacy, owing to the power imbalance between data processers (both Government and private) and individual users.[39] In this changed paradigm, it is in the interest of

---

> with the guarantees in Article 8 of the Convention. … Furthermore, when such disclosure has taken place, the positive obligation inherent in the effective respect of private life implies an obligation to carry out effective inquiries in order to rectify the matter to the extent possible.
>
> 75. In the present case the Court recalls that disclosures of a private nature inconsistent with Article 8 of the Convention took place. It follows that once the transcripts were deposited under the responsibility of the registry, the authorities failed in their obligation to provide safe custody in order to secure the applicant's right to respect for his private life. …. In fact, by reason of their failure to start effective investigations into the matter, the Italian authorities were not in a position to fulfil their alternative obligation of providing a plausible explanation as to how the applicant's private communications were released into the public domain.
>
> 76. The Court holds, therefore, that the respondent State did not fulfil its obligation to secure the applicant's right to respect for his private life and correspondence. There has consequently been a violation of Article 8 of the Convention.).

[38] *Subramanian Swamy v. Union of India & Ors.*,Writ Petitioner (Criminal) no. 184/2014, decided on May 13, 2016.

[39] Ujwala Uppaluri, *Digital Memory & Informational Privacy: Reflecting on the EU's 'Right to be Forgotten' – Working Paper by Ujwala Uppaluri*, CENTRE FOR COMMUNICATION GOVERNANCE AT NATIONAL LAW UNIVERSITY, DEHLI (2015), https://ccgnludelhi.wordpress.com/2015/06/24/digital-

both private corporations and civil society to adopt legal regimes which are transparent and inspire trust in individual users of the internet.[40]

It is worth noting that privacy does not necessarily require a complete absence of information pertaining to an individual in the public domain, but rather an individual's right to effectively control the information that relates to him or her. In other words, the right to privacy entails an individual's right to self-determination, or an individual's right to control his or her identity in cyberspace.[41] There are two aspects to this right:[42]

- Information about an individual should not be automatically made available to other individuals and organizations; and

- An individual must be able to exercise a substantial degree of control over the information provided by him or her and its use.

This highlights the need to regulate all aspects of data collection and use, including what can be collected, who it can be collected from, how it can be put to use, and what measures must be adopted by those collecting such data to protect it. Formulating strong and enforceable data protection standards is very important for a developing economy such as India's, which has found its feet in the global economy by leading the market in outsourcing and processing data from companies around the world,[43] and is seeking to position itself as an attractive destination for businesses.[44]

Data Protection in Other Jurisdictions

In the European Union, data protection is governed by the Data Protection Directive.[45] This Directive provides for the establishment of the Data Protection Authority (DPA), which is capable of investigating privacy concerns and enforcing the mandate of the Directive. Importantly, it permits the transfer of personal data from

---

memory-informational-privacy-reflecting-on-the-eus-right-to-be-forgotten-working-paper-by-ujwala-uppaluri/.

[40] Justice Ajit Prakash Shah, *Report of the Group of Experts on Privacy*, PLANNING COMMISSION OF INDIA (2012), http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf.

[41] Uppaluri and Shivanagowda, *Preserving Constitutive Values*, *supra* note 9.

[42] Dr. Shiv Shankar Singh, *Privacy and Data Protection in India*, (2012) PL February S-2.

[43] *First Analysis of the Personal Data Protection Law in India*, CRID – UNIVERSITY OF NAMUR (2005), http://ec.europa.eu/justice/data-protection/document/studies/files/final_report_india_en.pdf.

[44] David J. Kessler, Sue Ross, and Elonnai Hickok, *A Comparative Analysis of Indian Privacy Law and the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules*, 26 NLSI REV. 31 (2014).

[45] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data on the Free Movement of Such Data.

a member state to a country outside the European Union only if the destination country offers "an adequate level of protection."[46]

However, since the adoption of the Data Protection Directive in 1995, there have been substantial advances in information technology and the manner in which information is exchanged on the internet. Therefore, the European Union has been working towards enacting a harmonised legislation, the General Data Regulation,[47] which will replace the Data Protection Directive. The Regulation was adopted by the European Council on April 8, 2016,[48] and by the European Parliament on April 14, 2016.[49] Among other things, the Regulation is an endeavour to further ensure accountability of data controllers, extend liability beyond data controllers to include data processors as well, bring about uniformity in the sanctions prescribed, and rework the regulatory framework by providing for supervisory authorities.[50]

In the United States, rather than protecting all personal data with omnibus legislation, privacy laws are sectoral, with different laws regulating different industries.[51] While there is no overarching federal law that directly concerns the data collected and used by online merchants, such as Amazon.com or social media platforms such as Facebook, the privacy interests of individuals with respect to such data are protected by the Federal Trade Commission's enforcement of federal privacy and consumer protection policies.[52]

Data Protection in India

Similarly, India does not have holistic legislation that deals with the protection of data, and has instead adopted the sectoral approach. There are over fifty sectoral laws, policies, and regulations that contain provisions relevant to privacy,[53] including

---

[46] *Id*.

[47] COM(2012) 11 final, Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), Eur. Comm'n H.R. (Jan. 1, 2012),http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

[48] Reform of the EU Data Protection Rules, Eur. Comm'n H.R., http://ec.europa.eu/justice/data-protection/reform/index_en.htm.

[49] Joint Statement on the Final Adoption of the New EU Rules for Personal Data Protection, Eur. Comm'n H.R. (Apr. 14, 2016), http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm.

[50] *The Proposed EU General Data Protection Regulation: A Guide for In-House Lawyers*, Hunton & Williams (June 2015), https://www.huntonregulationtracker.com/files/Uploads/Documents/EU%20Data%20Protection%20Reg%20Tracker/Hunton_Guide_to_the_EU_General_Data_Protection_Regulation.pdf.

[51] Daniel J. Solove and Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUMBIA L. REV. 583 (2013).

[52] *Id*.

[53] Kessler, Ross, and Hickok, *A Comparative Analysis*, *supra* note 44.

legislation in the financial[54] and health[55] sectors. In the context of the internet and digital information, the Information Technology Act 2000 provides the existing framework for privacy protection. This is, in part, reflective of the lack of awareness of and emphasis on privacy interests in India.[56] In the United States, privacy is widely understood in the context of financial information and identity theft, whereas in India, "privacy" is still construed in terms of personal space.[57] Evidence gathered from throughout the world suggests that consumers do not read or understand privacy policies, are heavily influenced by the way choices are framed, and harbor many pre-existing assumptions that are incorrect.[58]

Scope of "Data" Protected

In India, the provisions of the Information Technology Act 2000 apply to any data that is collected or processed in India. "Data" is defined as "a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer."[59] Information "includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche."[60]

The provisions of the Information Technology Act 2000 did not reference "personal information" until 2011, when the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 were notified. In these Rules, "personal information" is defined as "any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate or individuals acting on its behalf (collectively referred to as "the body corporate"), is capable of identifying such person."[61] Evidently, this is a very broad definition, and

---

[54] For example, Chapter VI (Sections 19 to 22) of the Credit Information Companies (Regulation) Act 2005 lays down, in detail, the requirements that are to be complied with by a Credit Information Company while conducting its business.

[55] For example, Regulation 1.3 of the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations 2002 provides for the maintenance of medical records and the procedure to be followed while disclosing these records.

[56] Ponnurangam Kumaraguru and Niharika Sachdeva, *Privacy in India: Attitudes and Awareness . 2.0*, INDRAPRASTHA INSTITUTE OF INFORMATION TECHNOLOGY (Nov.22, 2012), http://precog.iiitd.edu.in/research/privacyindia/PI_2012_Complete_Report.pdf.

[57] *First Analysis of the Personal Data Protection Law*, *supra* note 43.

[58] Solove and Hartzog, *The FTC and the New Common Law of Privacy*, *supra* note 51.

[59] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, Section 2(1)(o).

[60] *Id*. at Section 2(1)(v).

[61] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Gen. S. R. & O. 313(E) (India), Rule 2(1)(i).

the Rules go on to define "sensitive personal data or information" relating to a person as "personal information which relates to passwords, financial information such as Bank account or credit card or debit card or other payment instrument details, physical, physiological and mental health conditions, sexual orientation, medical records and history, biometric information, any detail relating to the above as provided to body corporate for providing service, any of this information received by body corporate for processing, stored or processed under lawful contract."[62] The only exceptions provided for by the Rules concern information that is freely available in the public domain, information furnished under the Right to Information Act 2005, or as provided under any other law in force.[63]

Intermediaries' Liability with Respect to Data

The provisions in the IT Act 2000, which deal with the primary liability of a body corporate or an individual that collects and handles data, may be viewed under two heads:

- Liability which arises out of negligence in maintaining reasonable security practices and procedures to safeguard data, where such negligence results in wrongful loss to any person.

In this regard, Section 43A[64] of the IT Act 2000 requires that intermediaries maintain reasonable security practices and procedures, and failure to do so which results in

---

[62] *Id*. at Rule 3.

[63] *Id*.

[64] Section 43A - Compensation for failure to protect data

> Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.
>
> Explanation.-- For the purposes of this section,--
>
> (i) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;
>
> (ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;

wrongful loss or gain to any person will render such body corporate liable to the injured person for damages. Therefore, it appears that the standard applied to a body corporate that handles and collects data is not one of strict liability, but rather one of taking reasonable care to ensure that it maintains reasonable security practices and procedures. The Section goes on to explain that "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure, or impairment, as may be specified in any law, agreement between the parties, or prescribed by the Central Government.

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, define the practices and procedures that a body corporate must employ while handling sensitive personal data or information in order to ensure the security of such data or information.[65] Under these Rules, the body corporate shall be considered to have complied with reasonable security practices and procedures if it has implemented such security practices and standards, a comprehensive documented information security program, and information security policies, that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business.[66] In the event of a breach, the body corporate must be able to demonstrate that it has implemented reasonable security control measures in order to avoid liability.[67]

The Rules stipulate that the international standard IS/ISO/IEC 27001 on "Information Technology – Security Techniques – Information Security Management System – Requirements" is one such standard by which the reasonableness of security measures may be evaluated.[68] Furthermore, the body corporate must undergo an audit of its security practices on an annual basis.[69]

- Liability which arises out of the intentional disclosure of any personal information that is capable of identifying such person.

In this regard, Section 72A of the IT Act 2000 provides for criminal liability on any person (including an intermediary) who discloses the personal information of another person to any other person without the consent of the person concerned or in breach of a lawful contract, with intent to cause or knowing that he is likely to cause a wrongful loss or gain.[70]

(iii) "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

[65] Kessler, Ross, and Hickok, *A Comparative Analysis*, *supra* note 44.
[66] Information Technology Rules, *supra* note 61, at Rule 8(1).
[67] *Id*.
[68] *Id*. at Rule 8(2).
[69] *Id*. at Rule 8(4).
[70] IT Act, *supra* note 59, at Section 72A (Punishment for disclosure of information in breach of lawful contract:

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 reiterates that prior consent is required for disclosure of sensitive personal data or information, unless such disclosure has already been agreed to by contract or is necessary for compliance with a legal obligation.[71] The Rules also restrict a third party who is in receipt of any sensitive personal data or information from disclosing it further.[72]

Therefore, under the IT Act 2000, a person who has suffered a breach of personal data may seek a remedy under either Section 43A, which grants compensation for failure to implement reasonable security procedures, or under Section 72A, which provides for criminal liability for the defendant in cases where an intermediary secures personal information and discloses it without consent or in breach of contract, with the intent of causing wrongful loss or gain. Apart from these provisions, Section 45 provides for a residuary penalty of Rs. 25,000 for non-compliance with the provisions of the Act where no specific penalty has been defined.[73]

Obligations While Collecting and Handling Data

In the course of its operations, a body corporate that collects and handles "information" is required to create a privacy policy for the handling of or dealing in such personal information (including sensitive personal data or information), and to ensure that the policy is available for view by the user who is providing the information.[74] The privacy policy must provide for the following:

(i) Clear and easily accessible statements of its practices and policies;
(ii) the type of personal or sensitive personal data or information collected;
(iii) the purpose of collection and usage of such information;
(iv) how and why the information may be disclosed; and
(v) reasonable security practices and procedures

Furthermore, the Rules contain provisions which require a body corporate to take certain steps in order to protect the privacy rights of the individuals from whom the information is collected:

Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.).

[71] Information Technology Rules, *supra* note 61, at Rule 6(1).
[72] *Id*.at Rule 6(4).
[73] Kessler, Ross, and Hickok, *A Comparative Analysis*, *supra* note 44.
[74] Information Technology Rules, *supra* note 61, at Rule 4.

- **Choice & Consent**: The body corporate must obtain the consent of the person whose sensitive personal data or information is being collected regarding the purpose of collection and use of such information in writing through letter, fax, or email.[75]

- **Collection Limitation**: The body corporate may only collect sensitive personal data or information for a lawful purpose connected with a function or activity of the data controller, and only the information necessary for the purpose.[76]

- **Purpose Limitation**: Information collected must be used only for the purpose for which it was collected, and shall not be retained for longer than is required for the purpose.[77]

- **Access & Correction**: The body corporate must permit an individual to review the information they have provided, and ensure that any information found to be inaccurate or deficient is corrected or amended.[78]

- **Disclosure of Information**: The body corporate shall obtain permission from an individual prior to disclosing their sensitive personal data or information, unless the disclosure has been agreed to by contract or mandated by law. Any third party receiving the sensitive personal data shall not disclose it further, and shall ensure that the same level of data protection is made available. An exception is provided for sharing the information with Government Agencies without obtaining prior consent, if such disclosure is mandated by law for the purpose of verification of identity, prevention, detection, and investigation of offences.[79]

- **Accountability**: A Grievance Officer must be appointed by the data controller in order to address any discrepancies and grievances raised by an individual with respect to the information provided by him.[80]

Review of the Law on Privacy

The IT Act 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 put into place fairly detailed guidelines that dictate the operations of an intermediary while collecting and handling data. The introduction of these Rules in 2011 was primarily the result of privacy concerns raised when the telephonic conversations of Niira

---

[75] *Id*. at Rule 5(1), (7).
[76] *Id*. atRule 5(2).
[77] *Id*. at Rule 5(4),(5).
[78] *Id*. at Rule 5(6).
[79] *Id*. at Rules 6, 7.
[80] *Id*. at Rule 5(9).

Radia, a corporate lobbyist, with various industrialists and politicians were leaked to the press.[81] Nevertheless, driven by concerns that the these provisions were insufficient to deal with broad privacy concerns in the context of the modern internet, a Group of Experts on Privacy[82] was constituted by the Planning Commission of the Government of India to identify key privacy issues and prepare a foundation for a new Privacy Bill aligned with the international landscape of privacy laws, global data flows, and privacy concerns that have arisen with rapid technological advancements.

After analysing the international law pertaining to privacy[83] and comparing it with the existing privacy jurisprudence in India, the Expert Group published a 92–page report making recommendations to streamline the law pertaining to data protection and privacy in India.[84] At the outset, the Group of Experts recognized that the need for regulation stems from the economic value of data, and that global data flow generates value for the individual as a data creator and for businesses that collect and process such data. Therefore, the Expert Group stated that the objective "should [be to] put into place a regulatory framework for both public and private sector organizations. The ambit of the privacy legislation will extend to data being processed within India, and data that originated in India, even when it is transferred internationally."[85]

Drawing from international best practices, the Group of Experts recommended that legislation on privacy must recognize the constitutional basis of the right to privacy, and documented the nine fundamental principles that would form the bedrock of the proposed privacy legislation: notice, choice and consent, collection limitation, purpose limitation, access and correction, disclosure of information, security, openness, and accountability. Further, the Group of Experts asserted that the validity of any exception to the right to privacy should be judged against the following principles:[86]

- Proportionality: the limitation should be proportionate to the harm that has been or will be caused.

---

[81] ITDG Bureau, *India needs law against invasion of privacy: Ratan Tata*, INDIA TODAY (Feb. 16, 2011), http://indiatoday.intoday.in/story/india-needs-law-against-invasion-of-privacy-ratan-tata/1/130050.html.

[82] The Group of Experts on Privacy was chaired by Justice AP Shah, former Chief Justice of the Delhi High Court, and its members included representatives from the Planning Commission and the Department of Personnel & Training under the Government of India, industry bodies such as NASSCOM and DSCI, academia and research centres such as Centre for Internet and Society, and media outlets such as NDTV.

[83] Including the OECD Privacy Guidelines, EU Data Protection Directives, APEC Privacy Framework, Canada Personal Information Protection and Electronic Documents Act (PIPEDA), and Australia National Privacy Principles (ANPP).

[84] Justice Ajit Prakash Shah, *Report of the Group of Experts on Privacy*, PLANNING COMMISSION OF INDIA (2012), http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf.

[85] *Id*.

[86] *Id*.

- Legality: the limitation should be in accordance with the laws of the land.

- Necessary in a Democratic State: the limitation should extend only to the extent it is necessary in a democratic state.

It was recognized that the fundamental philosophy underlying these principles is the need to ensure transparency, enforceability, and accountability for the collection, processing, and use of data, thereby ensuring that the privacy of the concerned individual is guaranteed. The conception of the Privacy Principles by the Group of Experts appears to be a departure from the "third party doctrine" in the U.S., and is based on the idea that the information forms a part of the individual and his dignity, and therefore ought to be protected.

While the existing provisions contained in the IT Act and Rules do serve to achieve the ends of the nine Privacy Principles to some extent, the Group of Experts identified and recommended a number of ways in which the Privacy Bill could improve upon the laws relating to data protection. Among other measures, the Group recommended that the proposed privacy legislation should apply to both the private and public sectors, and to all data processed in India even if it is subsequently transferred to another jurisdiction.[87]

The Group of Experts also identified several lacunae in the existing law governing data protection by giving effect to the nine Privacy Principles. For instance, they noted the widespread practice of correlating data subjects' profiles with other available third party sources to build a comprehensive data profile of the subject without their knowledge.[88] Some pertinent recommendations made by the Group of Experts in regard to this practice are that:

- changes in privacy policy should be notified to the public and the individual;
- information should be destroyed once it has been used in accordance with the identified purpose; and
- data controllers must provide notice of disclosure to third parties.

Finally, the Group of Experts placed great emphasis on the last of the Privacy Principles. The Group's focus on "accountability" was premised on a rejection of the "one size fits all" approach and based instead on the belief that implementation of the Privacy Principles can only be effective through regulations that focus on the outcome, while leaving the precise mode and manner of implementation to be determined by each organization.[89]

---

[87] *Id*.
[88] *Id*.
[89] *Id*.

Therefore, the Group opined that the existing system of designating a Grievance Officer under Rule 5(9) of the IT Rules 2011 was entirely unsatisfactory. They recommended that a two-fold regulatory mechanism be adopted in its place: (i) establishing an office of the Privacy Commissioner at the central and regional levels, who would have the power to investigate class action complaints or complaints received from individuals, and (ii) encouraging data controllers to achieve self-regulation by setting up Self-Regulating Organisations (SROs) that would be vested with the responsibility of autonomously ensuring compliance with the Act, who themselves would be subject to oversight by the Privacy Commissioner.

Under this approach, all data controllers are free to develop their own systems that are suited to the environments in which they operate. In such a framework, if and when a breach occurs, it is the responsibility of the data controller to prove that it performed due diligence and adhered to all the Privacy Principles in the course of its functioning.

Privacy Bill 2014

Based on the recommendations of the Group of Experts, the Government has attempted to rework the privacy and data protection laws in India by preparing a draft Right to Privacy Bill 2014.[90] Heeding the recommendation of the Group of Experts, the Bill explicitly recognizes that the right to privacy is a part of the right to life under Article 21 of the Constitution. The nine Privacy Principles are enumerated in the Schedule to the Bill, and its provisions give effect to the Principles in such a way that elevates the data protection law in India to be virtually on par with the regime in Europe, and requires that all personal data mandatorily disclosed to intermediaries be processed according to the Bill.[91]

The Privacy Bill will apply to any person who "shall collect, process, or otherwise deal with personal data of any individual" (all residents of India, and not merely citizens of India). A data controller who does not maintain a place of business in India but who collects and handles the personal data of any Indian resident must nominate a representative resident in India who will be responsible for compliance. It is unclear whether all overseas data controllers who collect data from residents in India may be compelled to nominate a representative resident in India[92] or the consequences if a data controller fails to appoint such a representative.

---

[90] The draft Privacy Bill 2014 has not yet been made public. For analytical purposes, this Report has relied on articles written by CIS discussing the provisions of the Privacy Bill. *See, e.g.*, Elonnai Hickok, *Leaked Privacy Bill: 2014 vs. 2011*,THE CENTRE FOR INTERNET AND SOCIETY (Mar. 31, 2014), http://cis-india.org/internet-governance/blog/leaked-privacy-bill-2014-v-2011.

[91] Graham Greenleaf, *India's draft The Right to Privacy Bill – Will Modi's BJP Enact It?*, 129 PRIVACY LAWS & BUSINESS INTERNATIONAL REPORT 21 (2014), http://ssrn.com/abstract=2481796.

[92] *Id*.

For the purpose of enforcement, the Bill envisages the creation of a Data Protection Authority (DPA), which will have strong powers to investigate the actions of data controllers and to issue directives in relation to the discharge of any of its functions. The Bill also contains general provisions that provide for "industry associations" to develop "privacy standards" consistent with the Bill, and to appoint an industry-specific ombudsman. Consequently, any aggrieved person may make a complaint to the Privacy Officer of the data controller, to the ombudsman of the relevant industry association, or even directly to the DPA.

Secondary Liability

Intermediaries are a crucial cog in the machinery of the internet that allows people around the world to communicate with each other[93] by exercising their freedom of speech. However, the content posted by users and hosted by intermediaries may fall afoul of the law, a problem that is compounded by the open structure of the internet and its wide reach. For example, the posting of unauthorized content may give rise to a claim of copyright infringement, disparaging and false content can lead to a claim of defamation, and in some cases the exercise of one's right to free speech may transcend the permissible limit and result in the infringement of another's privacy.

In India, the debate on intermediary liability based on hosted content arose when Avnish Bajaj, the CEO of the auction portal Baazee.com, was arrested after a user posted an obscene multimedia clip for sale on the site. While dismissing a motion to quash the proceedings at the outset, the Delhi High Court held that the website which hosted such material could be held liable under Section 67 of the IT Act 2000 for publishing information which is obscene in electronic form.[94]

The Avnish Bajaj case resulted in the amendment of the Information Technology Act 2000, in order to allow intermediaries to incorporate safeguards to protect against liability based on content hosted by them. On this issue, due to the anonymous nature of the internet, it is often argued that intermediaries are best placed to filter or take down such objectionable content, since they possess the technical means to do so. However, fixing liability on intermediaries for the content they host must be viewed in the context of the freedom of the speech. The fact that intermediaries have the means to prevent access to content does not mean that they are best placed to evaluate whether the content in question is illegal. Consequently, leaving the task of regulating content entirely to intermediaries, in the absence of sufficient guidelines and safeguards, could have a "chilling effect" on free speech and expression.[95]

---

[93] Article 19 Free Word Centre, *Internet Intermediaries*, *supra* note 5.
[94] *Avnish Bajaj v. State*, 150 (2008) DLT 769.
[95] Felix T. Wu, *Collateral Censorship and the Limits of Intermediary Immunity*, 87 NOTRE DAME L. REV. 293 (2013).

Nevertheless, the question is no longer whether the intermediary should be liable for the content hosted by it, but rather the circumstances under which an intermediary should be held liable for third-party content hosted and disseminated by it. This requires balancing various competing interests, including individuals' privacy interest, intermediaries' operations, and third parties' right to free speech.

Freedom of Speech

Article 19 of the Universal Declaration of Human Rights (UDHR)[96] guarantees the right to freedom of expression as the right to "hold opinions without interference and to seek, receive, and impart information and ideas through any media and regardless of frontiers." Article 19 of the International Covenant on Civil and Political Rights (ICCPR) echoes and gives force to the right in more elaborate terms.[97] Article 19 of the ICCPR was clarified by the UN Human Rights Committee in September 2011,[98] which stated that Article 19 of ICCPR "protects all forms of expression and the means of their dissemination … including all forms of electronic and internet-based modes of expression … State parties should take account of the extent to which developments in information and communication technologies, such as internet and mobile based electronic information dissemination systems, have substantially changed communication practices around the world. There is now a global network for exchanging ideas and opinions that does not necessarily rely on the traditional mass media intermediaries. State parties should take all necessary steps to foster the independence of these new media and to ensure access of individuals thereto."

---

[96] G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948).

[97] G.A. Res. 2200 (XXI) A, International Covenant on Civil and Political Rights (Dec. 16, 1966), Article 19 (The relevant portion of this text is as follows:

1. Everyone shall have the right to hold opinions without interference.

2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

    (a) For respect of the rights or reputations of others;

    (b) For the protection of national security or of public order (ordre public), or of public health or morals.).

[98] *Id*. at General Comment No. 34, http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf.

However, the right to freedom of expression is not an absolute right, as Article 19(3) permits restrictions that are necessary (a) for respect of the rights or reputation of others, and (b) for the protection of national security or public order, or of public health or morals, but such restriction must be provided by law. A restriction on the right to freedom of expression will be permissible if it (i) is provided by law, (ii) pursues a legitimate aim, and (iii) conforms to the test of necessity and proportionality. These restrictions are applicable to any restrictions of the right exercised on the internet, as noted by the UN Human Rights Committee:[99]

> "Any restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3. Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with paragraph 3. It is also inconsistent with paragraph 3 to prohibit a site or an information dissemination system from publishing material solely on the basis that it may be critical of the government or the political social system espoused by the government."

The approach to regulating intermediaries with respect to the content hosted by them in a particular jurisdiction is largely dependent on the extent to which freedom of speech is protected in the relevant jurisdiction. For example, in the United States, the freedom of speech is virtually absolute,[100] whereas in India the freedom of speech is subject to certain reasonable restrictions imposed by the State.[101]

Strict Liability

One approach is the strict liability model, applied in China and Thailand, where intermediaries are strictly liable for third-party content hosted by them.[102] Under this model, intermediaries must actively monitor their hosted content in order to comply with the law, and failure to do so entails a variety of sanctions, including business penalties.

However, the general international consensus is that intermediaries should not be held to a standard of strict liability for unlawful content published by a third party of which

---

[99] *Id.*
[100] U.S. CONST. amend. I.
[101] INDIA CONST., art. 19.
[102] Article 19 Free Word Centre, *Internet Intermediaries*, *supra* note 5.

the intermediary is not aware.[103] This consensus appears to be based on the fact that it is not desirable for the intermediary to adopt an active role in monitoring and blocking data or content it hosts. Such a requirement may be so economically burdensome that all intermediaries would eventually shut up shop, greatly harming the growth of the internet, and in turn public interest. Furthermore, as discussed earlier, by assigning liability to intermediaries for all unlawful content published on their platforms by third parties, intermediaries are incentivised to engage in expansive censorship in order to avoid expensive litigation,[104] whether or not the speech is lawful.

"Safe Harbour"

The other approach is the "safe harbour" model, which provides immunity to intermediaries if they comply with certain requirements.[105] Under this model, the liability of an intermediary with respect to illegal or offensive content hosted by it is dependent upon the role played by the intermediary in distributing such content (e.g., whether it is active or passive). An intermediary that is aware of the content made available by it, and which exercises control over such content by editing it, is much more likely to be held liable for such content.

In the United States, the safe harbour model is primarily applied to intermediaries with respect to copyright issues.[106] However, a different approach is used for defamatory or offensive content,[107] thereby preventing online intermediaries from being treated as the publisher of user content that gives rise to claims of defamation, invasion of privacy, tortious interference, and general negligence.

Intermediary Liability in India

India adopted the conditional "safe harbour" approach in 2008 by amending the Information Technology Act 2000 to modify the safe harbour provision contained in Section 79. Under the amended statute, an intermediary is only liable for infringing or offensive content if it is established that the intermediary was notified of the content and subsequently failed to take steps to take it down. If an intermediary does not fall

---

[103] Gavin Sutter, *Rethinking Online Intermediary Liability: In Search of the 'Baby Bear' Approach*, 7 INDIAN J. OF LAW AND TECHNOLOGY 33 (2011), http://ijlt.in/wp-content/uploads/2015/08/gavin_sutter2.pdf.

[104] Chinmayi Arun, *Gatekeeper Liability and Article 19(1)(a) of the Constitution of India,* WORKING PAPER SERIES, CENTRE FOR COMMUNICATION GOVERNANCE AT NATIONAL LAW UNIVERSITY DELHI (May 20, 2015), http://ssrn.com/abstract=2643278.

[105] Article 19 Free Word Centre, *Internet Intermediaries*, *supra* note 5.

[106] Digital Millennium Copyright Act, Pub. L. 105-304 §512 (1998).

[107] Communications Decency Act, 47 U.S.C. §230.

within the safe harbour, it may incur civil or criminal liability for defamation, obscenity, sedition, or other actions.[108]

Section 79 of the IT Act 2000 provides that "an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him."[109] This protection from liability is not absolute, and is subject to the conditions laid down in Sub-Section (2) of Section 79:

- The function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted;

---

[108] Chinmayi Arun and Sarvjeet Singh, *Online Intermediaries in India*, NOC Online Intermediaries Case Studies Series (February 18, 2015), available at SSRN: http://ssrn.com/abstract=2566952.

[109] IT Act, *supra* note 59, at Section 79 (Exemption from liability of intermediary in certain cases

(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.

(2) The provisions of sub-section (1) shall apply if-

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or

(b) the intermediary does not-
(i) initiate the transmission,
(ii) select the receiver of the transmission, and
(iii) select or modify the information contained in the transmission;

(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

(3) The provisions of sub-section (1) shall not apply if-

(a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act;

(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Explanation - For the purposes of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.).

- the intermediary does not initiate the transmission, select the receiver of the transmission, or select or modify the information contained in the transmission; and

- the intermediary observes due diligence while discharging its duties under the Act, and observes the guidelines prescribed by the Central Government in this respect.

Furthermore, Subsection (3) provides for two exceptional situations in which the safe harbour provision under Section 79(1) will not apply. The first exception, under Section 79(3)(a). is for cases where the intermediary has conspired, abetted, aided, or induced the commission of the unlawful act. The second exception, contained in Section 79(3)(b), is an incorporation of the "notice and takedown" approach. It provides that the safe harbour provision shall not apply if, "upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner."

The modalities of the "notice and takedown" regime are provided in the Information Technology (Intermediaries Guidelines) Rules 2011, which were notified by the Government of India on April 11, 2011.[110] Rule 3 provides that an intermediary "shall not knowingly host or publish any information or shall not initiate the transmission, select the receiver of the transmission, and select or modify the information," and casts an obligation on the intermediary to disable such information within thirty-six hours of it being brought to the intermediary's attention by any affected person.[111]

---

[110] Information Technology (Intermediaries Guidelines) Rules, 2011, Gen. S. R. & O 314(E) (India).

[111] *Id*. at Rule 3 (Due diligence to be observed by intermediary — The intermediary shall observe following due diligence while discharging his duties, namely:

(2) Such rules and regulations, terms and conditions or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that —
  (a) belongs to another person and to which the user does not have any right to;
  (b) is grossly harmful, harassing, blasphemous defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever;
  (c) harm minors in any way;
  (d) infringes any patent, trademark, copyright or other proprietary rights;
  (e) violates any law for the time being in force;
  (f) deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature;
  (g) impersonate another person;

The "notice and takedown" mechanism has faced criticism from international bodies[112] as being unfair and apparently lacking any clear legal basis, as it requires the intermediary to remove unlawful material merely on the request of a private party or the State. This creates a situation where intermediaries will tend to "over-regulate" the internet, and material taken down may be perfectly legitimate and lawful.

One solution to this problem is to require the intermediary to remove unlawful content only upon receiving an order from the Court. For instance, this concern seems to have been addressed in the framework of the notice and takedown mechanism under the Copyright Act 1957, by requiring that intermediaries block content for a temporary period of twenty-one days only, beyond which it can restore access if the complainant has not procured an order from a competent court.[113]

(h) contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource;

(i) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting any other nation.

(3) The intermediary shall not knowingly host or publish any information or shall not initiate the transmission, select the receiver of transmission, and select or modify the information contained in the transmission as specified in sub-rule (2):

provided that the following actions by an intermediary shall not amount to hosing, publishing, editing or storing of any such information as specified in sub-rule: (2) —

(a) temporary or transient or intermediate storage of information automatically within the computer resource as an intrinsic feature of such computer resource, involving no exercise of any human editorial control, for onward transmission or communication to another computer resource;

(b) removal of access to any information, data or communication link by an intermediary after such information, data or communication link comes to the actual knowledge of a person authorised by the intermediary pursuant to any order or direction as per the provisions of the Act;

(4) The intermediary, on whose computer system the information is stored or hosted or published, upon obtaining knowledge by itself or been brought to actual knowledge by an affected person in writing or through email signed with electronic signature about any such information as mentioned in sub-rule (2) above, shall act within thirty six hours and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule (2). Further the intermediary shall preserve such information and associated records for at least ninety days for investigation purposes.).

[112] U.N. Special Rapporteur, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue*, U.N. Doc. A/HCR/17/27 (May 16, 2011).

[113] Sections 52(1)(b) and (c) of the Copyright Act, 1957 contain a fair use model with respect to content that infringes copyright. They provide that the transient or incidental storage of a work or performance will not amount to infringement, if (i) it is purely in the technical process of electronic transmission or communication to the public, or (ii) if it is for the purpose of providing electronic links, access or integration. The former scenario is a blanket exemption from liability that arises out of "caching" and transmission by internet service providers, whereas the latter is not available as a

In *Shreya Singhal v. Union of India*,[114] the landmark case that dealt with the State's power to regulate content on the internet, one of the challenges was against Section 79(3)(b) of the IT Act 2000, on the ground that it requires the intermediary to exercise its own judgment upon receiving actual knowledge that any information is being used to commit unlawful acts. Furthermore, it was argued that any restrictions on the ability of intermediaries to host content would have an immediate, direct, and adverse bearing on internet users' freedoms under Article 19(1)(a).[115]

While the Supreme Court refused to strike down the provision altogether, the Court read it down to mean that the intermediary will be liable if "upon receiving actual knowledge that a court order has been passed asking it to expeditiously remove or disable access to certain material must then fail to expeditiously remove or disable access to that material …otherwise it would be very difficult for intermediaries like Google, Facebook, etc. to act when millions of requests are made and the intermediary is then to judge as to which of such requests are legitimate and which are not."[116]

Weathering State Intervention

Apart from concerns that arise when data is collected and used by private entities, the Government's use of data also requires regulation, including when the Government collects and stores data for electoral databases and universal identity cards, as well as cases where the Government intercepts data of private entities.

This dynamic exists because in India, the constitutional jurisprudence on the right to privacy suggests that it is subject to reasonable restrictions, if such restrictions are in furtherance of the interest of the security of the State. Any such action is bound to conflict with internet users' right of privacy; although such situations are not yet frequent occurrences in India, the possibility of State intervention similar to that seen in instances across the world looms large.

Intermediaries operating in India are subject to myriad laws and mechanisms which permit State oversight over the content hosted by them. In "The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for

---

defence to infringement if the intermediary "is aware or has reasonable grounds for believing that such storage is of an infringing copy." If not for the safe harbour protection contained in Sections 52(1)(b) and (c) of the Copyright Act 1957, intermediaries could be liable under Section 51(a)(ii) for secondary infringement as a person who provides any place to be used for communication of work to the public for profit, where such communication constitutes a copyright infringement.

[114] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

[115] J. Sai Deepak, *India: Intermediary liability regime, a historic opportunity missed by the Supreme Court*, INFORRM'S BLOG (Apr. 7, 2015), https://inforrm.wordpress.com/2015/05/13/india-intermediary-liability-regime-a-historic-opportunity-missed-by-the-supreme-court-j-sai-deepak/.

[116] *Shreya Singhal*, *supra* note 114.

Human Rights" (OHCHR), emphasis has been placed on the role played by private intermediaries in facilitating surveillance:[117]

> "There is strong evidence of a growing reliance by Governments on the private sector to conduct and facilitate digital surveillance. On every continent, Governments have used both formal legal mechanisms and covert methods to gain access to content, as well as to metadata. This process is increasingly formalized: as telecommunications service provision shifts from the public sector to the private sector, there has been a "delegation of law enforcement and quasi-judicial responsibilities to Internet intermediaries under the guise of 'self-regulation' or 'co-operation.'"

Unless the Government's ability to intervene is restrained, intermediaries may find themselves in a bind, attempting to balance compliance with the Government on the one hand and securing the privacy interests of their users on the other.

The IT Act 2000 contains provisions which vest in the Government the power to issue directions to intercept, monitor, and collect information that flows through "computer resources." Section 69 empowers the Government to "direct any agency of the appropriate Government to intercept, monitor, or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource," if it finds that it is necessary or expedient to do so in the interest of "the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence." In addition, Section 69B empowers the Government to "monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource," in order to "enhance cyber security and for identification, analysis and prevention of intrusion or spread of computer contaminant in the country." "Traffic data" has been defined in Explanation (ii) to Section 69B as "any data identifying or purporting to identify any person, computer system or computer network or any location to or from which communication is or may be transmitted."

An examination of these provisions suggests that the purpose for which the power under either of these sections may be exercised is different. The power to intercept data may be exercised by the Government when it is necessary or expedient to do so in the interest of the State, whereas the power to monitor and collect information can

---

[117] U.N. High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (2014).

be exercised for a range of purposes relating to "cyber security,"[118] which includes "identifying or tracking any person who has breached, or is suspected of having breached or being likely to breach cyber security."[119] This latter power appears wider than the power to intercept data, because "cyber security incident" has been defined to mean "any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly acceptable security policy resulting in unauthorized access, denial of service, disruption, unauthorized use of a computer resource for processing or storage of information, or changes to data or information without authorization."[120]

Importantly, in either case, any person in charge of the computer resource, including an intermediary, is required to cooperate and provide all requested facilities and technical assistance to the Government agency when such an order is issued by the Government,[121] and imposes criminal sanctions on any person who fails to assist the agency.[122] The intermediary is also required to designate an officer to receive and handle all requests and directions for interception, monitoring, or decryption of information generated, transmitted, received, or stored in any computer resource. [123] Where decryption is requested, the intermediary must assist the Government in decryption to the extent that the intermediary has control over the decryption key.[124]

Furthermore, the rigours of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, which require obtaining the permission of the individual prior to the disclosure of sensitive personal information, are not applicable in cases where information is sought by Government agencies under the mandate of a law.[125] All that is required is a written request from the Government agency and a statement that the information so obtained shall not be published or shared with any other person.[126]

Another means by which the Government may interfere with the privacy rights of an intermediary's users is by exercising the power to intercept Call Data Records. Clause 41.10 of the UAS License Agreement (as amended in June 2013)[127] requires all

---

[118] Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009, Gen. S. R. & O. 782(E) (India), Rule 3.
[119] *Id*. at Rule 3(f).
[120] *Id*. at Rule 2(f).
[121] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, Sections 69(3), 69B(2).
[122] *Id*. at Sections 69(4), 69B(4).
[123] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, Gen. S. R. & O. 780(E) (India), Rule 14.
[124] *Id*. at Rule 13(3).
[125] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Gen. S. R. & O. 313(E) (India), Rule 6(1).
[126] *Id*.
[127] 41.10. The designated person of the Central/ State Government as conveyed to the Licensor from time to time in addition to the Licensor or its nominee shall have the right to monitor the telecommunication traffic in every MSC/ Exchange/*MGC/MG* or any other technically feasible point in

Telecom Service Providers (TSPs) to provide the Call Data Records handled by them to the Government security agencies, as required by them. The power to do so appears to stem from Section 5(2) of the Indian Telegraph Act 1885, which empowers the Government to intercept communications in furtherance of any of the following:

- Interests of sovereignty and integrity of India;
- security of the State;
- friendly relations in foreign states;
- public order; and
- prevention of incitement to commission of an offense.

The procedure for such interception is laid down in Draft Rule 419B, which provides for disclosure of message-related information and Call Data Records (CDRs) to Indian authorities. Such interception must be authorized by order of the Secretary, Government of India in the Ministry of Home Affairs, or the Secretary of a State Government who is in charge of the Home Department. It is worth noting that what is envisioned is the collection of metadata pertaining to communications, not the content of the communications itself.

---

the network set up by the LICENSEE. The LICENSEE should make arrangement for monitoring simultaneous calls by Government security agencies. The hardware at LICENSEE's end and software required for monitoring of calls shall be engineered, provided/installed and maintained by the LICENSEE at LICENSEE's cost. However, the respective Government instrumentality shall bear the cost of user end hardware and leased line circuits from the MSC/ Exchange/ *MGC/MG* to the monitoring centres to be located as per their choice in their premises or in the premises of the LICENSEE. In case the security agencies intend to locate the equipment at LICENSEE's premises for facilitating monitoring, the LICENSEE should extend all support in this regard including Space and Entry of the authorized security personnel. The Interface requirements as well as features and facilities as defined by the Licensor should be implemented by the LICENSEE for both data and speech. Presently, the LICENSEE should ensure suitable redundancy in the complete chain of Monitoring equipment for trouble free operations of monitoring of at least 210 simultaneous calls for seven security agencies." Along with the monitored call following records should be made available:

(i) Called/calling party mobile/PSTN numbers.

(ii) Time/date and duration of interception.

(iii) Location of target subscribers. For the present, Cell ID should be provided for location of the target subscriber. However, Licensor may issue directions from time to time on the precision of location, based on technological developments and integration of Global Positioning System (GPS) which shall be binding on the LICENSEE.

(iv) Telephone numbers if any call-forwarding feature has been invoked by target subscriber.

(v) Data records for even failed call attempts.

(vi) CDR (Call Data Record) of Roaming Subscriber.

The LICENSEE shall be required to provide the call data records of all the specified calls handled by the system at specified periodicity, as and when required by the security agencies.

These exceptions to the right to privacy have been recognized by the Group of Experts on Privacy as well, and they cautioned that the exceptions discussed above must be subject to the principles of proportionality, legality, and necessity in a democratic state to measure the extent and validity of the exception to the right.[128]

Recent developments do not appear to heed these recommendations, as evidenced by reports of the Central Monitoring System (CMS) created by the Government.[129] Previously, the Government was required to put in a request to the TSP in order to procure information pertaining to a particular individual; now the TSPs are entirely out of the picture and the CMS can access any information pertaining to communications at will.[130]

Although the establishment of the CMS may be justified on the basis of the provisions of the Telegraph Act 1885, the powers and limitations on the functioning of the CMS are not properly defined in the absence of any Rules. This is particularly unsettling in view of the fact that the CMS now occupies the position of an Orwellian eye at the helm of all communications that take place within India. These issues surrounding the functioning of CMS present a number of concerns that must be addressed as early as possible, as failing to do so places TSPs who fall under the definition of "intermediaries" between a rock and a hard place, facing active Government interception of the data handled by them on one hand and potential infringement of their users' right to privacy on the other.

Even though the Right to Privacy Bill 2014 is a significant step toward strengthening data protection law in India, it appears that intelligence agencies have been granted broad exemptions from the provisions of the Bill, for actions in the interest of the sovereignty, integrity, and security of India.[131] The only safeguard is that any infringement of a person's right to privacy by an intelligence agency is subject to judicial review, during which the intelligence agency must demonstrate that such action was necessary for the aforementioned purposes.[132] This provision appears to be in line with the law laid down by the Supreme Court on the right to privacy, as it is not an absolute right, but instead is subject to the interest of the State.

However, it is a matter of concern that the Home Ministry of the Government of India is not satisfied with this provision, and is pushing for a blanket exemption for

---

[128] Justice Ajit Prakash Shah, *Report of the Group of Experts on Privacy*, PLANNING COMMISSION OF INDIA (2012), http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf.

[129] Pranesh Prakash, *How Surveillance Works in India*, NEW YORK TIMES (Jul.10, 2013), http://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india/?_r=0.

[130] Maria Xynou, *India's Central Monitoring System (CMS): Something to Worry About?*, CENTRE FOR INTERNET & SOCIETY (2011), http://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about.

[131] Greenleaf, *India's draft*, *supra* note 91.

intelligence agencies.[133] It is no secret that history is filled with numerous instances of the State's abuse of such powers.[134] To make matters worse, intermediaries also find themselves at the heart of controversies examined by the Indian judiciary, despite the limited role played by them in such incidents. For example, in January 2015, the Supreme Court passed an interim order in an ongoing case that requires Google, Yahoo, and Microsoft to refrain from advertising or sponsoring any advertisement which would violate Section 22 of the Pre-Conception and Pre-Natal Diagnostic Techniques Act, 1994.[135]

Conclusion

The summation of the law on intermediary liability with respect to privacy presented by this Report suggests that India is moving in the right direction in order to achieve a balance between intermediaries' operations and individuals' right to privacy. Even though the constitutional status of the right to privacy in India is far from settled, the legislature has taken steps to ensure that proper safeguards are developed to keep up with the privacy concerns that arise in the context of the rapidly-advancing technologies that constitute an "intermediary." While the amendments to the Information Technology Act 2000 serve to achieve these ends to a certain extent, the privacy of an individual in cyberspace will only be truly secured when it is formally recognized and applied by the introduction of the Privacy Bill.

However, this proposed legislation is not without its gaps in coverage, which ideally will be resolved prior to it being passed. For instance, the validity of the provisions which provide for extraterritorial operation of the Act must be examined, and the means of enforcement against foreign entities need to be clearly laid down. Furthermore, the effect of such legislation on other sectors is not clear, which are governed by specific regulations. For example, the medical profession is governed by the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations 2002 that provide for the maintenance of medical records and the procedure to be followed when disclosing these records. The application of the privacy principles discussed in this Report to the medical field may not be desirable; for example, if doctors are required to destroy a patient's records after treatment, they will be left with no medical history to rely on for providing care in the future. Finally, the legislature must specify the extent to which the privacy principles will apply to data

---

[133] Aman Sharma, *Intelligence agencies demand blanket exemption from Right to Privacy Bill*, THE ECONOMIC TIMES (Mar. 17, 2015), http://articles.economictimes.indiatimes.com/2015-03-17/news/60212173_1_intelligence-agencies-privacy-bill-home-ministry.

[134] Prashant Iyengar, *IP Addresses and Expeditious Disclosure of Identity in India*, 9 INDIAN J. OF LAW AND TECHNOLOGY 1 (2013), http://ijlt.in/wp-content/uploads/2015/08/Prashant-Iyengar.pdf.

[135] *Sabu Mathew George v. Union of India*, (2015) 1 SCR 108.

held by the Government, as well as put in place adequate checks and balances to reign in the Government's ability to intercept or modulate content hosted by intermediaries.