IN THE SUPREME COURT OF INDIA

CIVIL ORIGINAL JURISDICTION

WRIT PETITION CIVIL NO.494 OF 2012

IN THE MATTER OF

JUSTICE KS PUTTASWAMY ..PETITIONER

VERSUS

UNION OF INDIA ..RESPONDENTS

WRITTEN SUBMISSIONS
OF TUSHAR MEHTA
ADDITIONAL SOLICITOR GENERAL OF INDIA

[FOR UIDAI & STATE OF MADHYA PRADESH]

IN THE SUPREME COURT OF INDIA

CIVIL ORIGINAL JURISDICTION

WRIT PETITION CIVIL NO.494 OF 2012

IN THE MATTER OF

JUSTICE KS PUTTASWAMY ...PETITIONER

VERSUS

UNION OF INDIA ...RESPONDENTS

INDEX

Written Submission of Tushar Mehta Additional Solicitor General of India

IN THE SUPREME COURT OF INDIA
CIVIL ORIGINAL JURISDICTION
WRIT PETITION CIVIL NO.494 OF 2012

IN THE MATTER OF

JUSTICE KS PUTTASWAMY ...PETITIONER

VERSUS

UNION OF INDIA ...RESPONDENTS

WRITTEN SUBMISSIONS ON BEHALF OF
UNIQUE IDENTIFICATION AUTHORITY OF INDIA (UIDAI)
BY TUSHAR MEHTA, ADDL. SOLICITOR GENERAL OF INDIA

1. The right to privacy is, though an inherent right, is only a common law right. Whenever and wherever the competent legislature has found it necessary, expedient or desirable to protect a person's privacy, it has done so by enacting a statute and thus, making a statutory right of privacy. Such common law right which can be protected based upon specific subjects may not be declared as fundamental right on the following grounds and also on the ground that there are no "judicially discernable and manageable standards" to ascertain and define privacy. Any view on the ground of privacy, if taken, by smaller benches, are per incurium and, therefore, not a good law:

Privacy has always been recognised as a "right". It is a very important and enforceable right but not a fundamental right.

i. That the ratio of **Kharak Singh vs State of Uttar Pradesh** [AIR 1963 SC 1295; 1964 SCR (1) 332] that "privacy" is not a fundamental right has not been expressly or impliedly overruled by subsequent judgments rendered by this Hon'ble court.

The subsequent judgments which elevates the 'right to privacy' as a fundamental right are *per incurium*

ii. That in view of the law which exists as on date there is no fundamental right to privacy guaranteed under Part III of the Constitution of India

including under Article 21. If this Hon'ble Court would "read" privacy in Part-III, it will amount to amending the Constitution though the omission to mention privacy in Part III is conscious.

iii. Neither the constituent assembly nor the Competent legislature exercising power of amendment of the Constitution have embodied right of privacy under Part III of the constitution and the omission clearly appears to be conscious.

Even by employing 'external aid' for interpreting i.e. Constitution assembly debates, the interpretation canvassed by the petitioners etc. that privacy is a fundamental right cannot be sustained, in as much as, the Framers of the Constitution expressly did not deem it fit expedient or appropriate to incorporate a right to privacy in Part III of the Constitution in their wisdom;

iv. The courts have always refrained from creating a new right adopting the process of interpretation since creating a "right" is not the prerogative of the courts, but that of the Competent legislature. Even in other jurisdiction, the Courts have refrained from "creating" a right by way of judicial law making;

v. Wherever, the legislature of other sovereign countries of the world deemed it fit to confer "privacy" with Constitutional status, they incorporated the same either by way of amendment to the Constitution or by way of adoption of the same through parliamentary process. In absence thereof the right to privacy is, at best, a 'common law right' and the same can only be conferred / protected by way of a statute made by the Competent legislature.

2. UIDIA respectfully adopts the aforesaid submission made by Union of India. However, in addition to the submissions made by union of India UADAI submits as under:-

I "Privacy" is inherently a vague and subjective concept – A vague concept which is incapable of any precise definition/contours cannot be conferred with a status of Constitutional fundamental right

3. It is respectfully submitted that the term "privacy" is inherently vague and subjective notion having different meaning for different individuals. Such a notion is incapable of being precisely defined and has rambling application to various aspect of human life depending upon the preconceived notions of each individual. It is submitted that such a vague concept whose contours cannot be precisely defined cannot be elevated to and/or conferred status of a Constitutional fundamental right as there would be no judicially discernable and manageable standards to control and enforce the said right.

4. It is submitted that world over, all the legal as well as social scholars and luminaries are ad-idem that privacy, as a concept, is elusively difficult to define. The definitional framework which may be required to ascertain the extent and origins of privacy within the Indian Constitutional law setup may further be difficult to ascertain. This concept of privacy has over the years remained with little or almost no authoritative explanation. In this context it would be relevant to refer to the view express by some scholar who have tried to define privacy.

i) Mr Richard B. Parker in his article "A Definition of Privacy," has stated as under:-

> *". . . privacy is control over when and by whom the various parts of us can be sensed by others. By "sensed," is meant simply seen, heard, touched, smelled, or tasted. By "parts of us," is meant the part of our bodies, our voices, and the products of our bodies. "Parts of us" also includes objects very closely associated with us. By "closely associated" is meant primarily what is spatially associated. The objects which are "parts of us" are objects we usually keep with us or locked up in a place accessible only to us."*

[Richard B. Parker, "A Definition of Privacy," Rutgers Law Review 27 (1974):

281]

ii) Rachel L. Finn, David Wright and Michael Friedewald of Fraunhofer Institute for Systems and Innovation Research, in their paper titled as "Seven Types of Privacy" stated as under:

> *"Privacy" is a key lens though which many new technologies, and most especially new surveillance technologies, are critiqued.*[1] ***However, "privacy" has proved notoriously difficult to define.*** *Serge Gutwirth says "The notion of privacy remains out of the grasp of every academic chasing it. Even when it is cornered by such additional modifiers as "our" privacy, it still finds a way to remain elusive."*[2] *Colin Bennett notes that "attempts to define the concept of 'privacy' have generally not met with any success".*[3] ***Legal scholars James Whitman and Daniel Solove have respectively described privacy as "an unusually slippery concept"***[4]***,*** *and "**a concept in disarray. Nobody can articulate what it means**"*[5]*. Furthermore, **Debbie Kaspar notes that "scholars have a famously difficult time pinning down the meaning of such a widely used term [and] ...most introduce their work by citing this difficulty**".*[6] *Helen Nissenbaum has argued that privacy is best understood though a notion of **"contextual integrity**", where it is not the sharing of information that is a problem, rather it is the sharing of information outside of socially agreed contextual boundaries.*
>
> ....
>
> ***Although a widely accepted definition of privacy remains elusive, there has been more consensus on a recognition that privacy comprises multiple dimensions**, and some privacy theorists have attempted to create taxonomies of privacy problems, intrusions or categories.*
>
> ...
>
> *However, these scholars' focus on the ways in which privacy can be infringed and the legal problem which must be solved is largely reactive. **They focus on specific harms which are already occurring and which must be stopped, rather than over-arching protections that should be instituted to prevent***

---

[1]David Lyon, Surveillance after September 11 (Cambridge: Polity Press, 2003).
[2]Serge Gutwirth, Privacy and the information age (Lanham, MD: Rowman & Littlefield, 2002), 30.
[3]Colin J. Bennett, Regulating Privacy: Data Protection and Public Policy in Europe and the United States (Ithaca NY: Cornell University Press, 1992).
[4]James Q. Whitman, "The Two Western Cultures of Privacy: Dignity Versus Liberty," The Yale Law Journal 113 (2004): 1153-54.
[5] Daniel Solve, "I've Got Nothing to Hide' and Other Misunderstandings of Privacy," San Diego Law Review 44 (2007): 758.
[6]Debbie V. S. Kaspar, "The Evolution (or Devolution) of Privacy," Sociological Forum 20 (2005): 72.

harms.

...

We also suggest that the fluidity of privacy as a concept may be an important aspect of its utility, since technological developments may introduce new types of privacy. ***As technologies develop and proliferate, various types of privacy which had not previously been considered or identified as under threat may become compromised****.*

...

*...****we propose that fluidity and flexibility are necessary to enable "privacy" to respond to technological changes. More precise conceptualisations, taxonomies and boundaries surrounding privacy, particularly in the legal field, may disrupt the use of privacy to protect individuals and groups from intrusions that impact upon their freedoms, fundamental rights and access to goods and services****."*

[Seven Types of Privacy - Rachel L. Finn David Wright Michael Friedewald, Fraunhofer Institute for Systems and Innovation Research]

iii) The academic Helen Nissenbaum, in the book 'Privacy in Context - Technology, Policy, and the Integrity of Social Life', has enunciated key concepts on the definitional exercise as:

*"****Almost as many who have taken up the subject of privacy in relation to information technology have declared it deeply problematic, referring not only to questions and disagreements about its value, benefits, and harms but to its conceptual morass.*** *Attempts to define it have been notoriously controversial and have been accused of vagueness and internal inconsistency-of being overly inclusive, excessively narrow, or insufficiently distinct from other value concepts.* ***Believing conceptual murkiness to be a key obstacle to resolving problems, many have embarked on the treacherous path of defining privacy****. As a prelude to addressing crucial substantive questions, they have sought to establish whether privacy is a claim, a right, an interest, a value, a preference, or merely a state of existence. They have defended accounts of privacy as a descriptive concept, a normative concept, a legal concept, or all three. They have taken positions on whether privacy applies only to information, to actions and decisions (the so called Constitutional rights to privacy), to*

special seclusion, or to all three. They have declared privacy relevant to all information, or only to a rarefied subset of personal, sensitive, or intimate information, and they have disagreed over whether it is a right to control and limit access or merely a measure of the degree of access others have to us and to information about us. They have posited links between privacy and anonymity, privacy and secrecy, privacy and confidentiality, and privacy and solitude.

Believing that one must define or provide an account of privacy before one can systematically address critical challenges can thwart further progress*....*

*... **Maintaining all these meanings while delineating a concept to support policy, moral judgment, and technical design seems a hopeless ambition.***

...

Those who recognise the perils of inclusiveness attempt to purify the concept by trimming away some of the inconsistency and ambiguity, declaring certain uses wrong or confused. ***This has meant disputing the proper application of privacy so called Constitutional case, or it has meant rejecting control over information as part of the meaning of privacy in favour of degree of access or visa-versa.****"*

[Helen Nissenbaum, Privacy in Context, Technology, Policy, and the Integrity of Social Life, Stanford University Press]

iv) Scholar Julie E. Cohen in an article in Harvard Law Review titled "What Privacy Is For" has stated as under: -

*"**Most privacy theorists have tended to think that the key to defining privacy lies in locating privacy's essence in one or another overarching principle** (such as liberty, inaccessibility, or control) and then offering finely parsed resolutions of the resulting conflicts between the principles and ordinary, everyday practices and expectations.* ***Definitions of privacy grounded in core principles, however, inevitably prove both over and under inclusive when measured against the types of privacy expectations that real people have.*** *For example, such definitions can't explain the widespread belief that sharing personal details with one's friends or one's airplane seatmate does not automatically equal sharing them with one's employer. In the real world, privacy expectations and behaviors are unruly and heterogeneous, persistently defying efforts to reduce them to neat conceptual schema.*

.....

The self has no autonomous, pre-cultural core, nor could it, because we are born and remain situated within social and cultural contexts. ***And privacy is not a fixed condition, nor could it be, because the individual's relationship to social and cultural contexts is dynamic. These realities do not weaken the case for privacy; they strengthen it.***

....

Subjectivity is a function of the interplay between emergent selfhood and social shaping; privacy, which inheres in the interstices of social shaping, is what permits that interplay to occur. ***Privacy is not a fixed condition that can be distilled to an essential core, but rather "an interest in breathing room to engage in socially situated processes of boundary management."****It enables situated subjects to navigate within preexisting cultural and social matrices, creating spaces for the play and the work of self-making."*

v) Scholar Adam Moore, in a Journal Of Social Philosophy, wrote an article titled as "Defining Privacy" wherein it was argued that if privacy exists in various fields, requiring varying degrees of protection, it would incongruent to define it within the Constitutional framework as one overarching. In the said article following was argued by Adam Moore:-

> *"**Privacy has been defined in many ways over the last few hundred years**.[7]Warren and Brandeis, following Judge Thomas Cooley, called it "the right to be let alone."[8]Pound and Freund have defined privacy in terms of an extension personality or personhood.[9]Legal scholar William Prosser separated privacy cases into four distinct but related torts. "Intrusion: Intruding (physically or otherwise) upon the solitude of another in a highly offensive manner. Private facts: Publicizing highly offensive private information about someone which is not of legitimate concern to the public. False light: Publicizing a highly offensive and false impression of another. Appropriation: Using another's name or likeness for some advantage*

---

[7]See Judith Wagner DeCew, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (Ithaca, NY and London: Cornell University Press, 1997), chaps. 1–4.

[8]See Thomas M. Cooley, *Cooley on Torts* (2nd ed., 1888); S. Warren and L. Brandeis, "The Right to Privacy," *The Harvard Law Review* 4 (1890): 193–220.

[9]Roscoe Pound, "Interests in Personality," *Harvard Law Review* 28 (1915): 343; and Paul A. Freund, "Privacy: One Concept or Many?" in *Privacy Nomos XIII*, ed. Roland Pennock and John W. Chapman (New York: Atherton Press, 1971), 182.

without the other's consent."[10]

Alan Westin and others have described privacy in terms of information control.[11]*Still others have insisted that privacy consists of a form of autonomy over personal matters.*[12]*William Parent argued that "[p]rivacy is the condition of not having undocumented personal knowledge about one possessed by others,"*[13] *while Julie Inness defined privacy as "the state of possessing control over a realm of intimate decisions, which include decisions about intimate access, intimate information, and intimate actions."*[14]

More recently, Judith Wagner DeCew has proposed that the "realm of the private to be whatever types of information and activities are not, according to a reasonable person in normal circumstances, the legitimate concern of others."[15]

.....

"I have maintained that privacy should be defined as a right to control access to places, locations, and personal information along with use and control rights to these goods. ***Nevertheless, it is likely the case that any definition of a right to privacy will not satisfy everyone. It is equally true that how the right is justified will play an important role in providing the dimensions of the definition at issue—thus, any attempt to define privacy rights independent of a justifying theory will likely be incomplete****."*

Adam Moore, Defining Privacy, Journal Of Social Philosophy, Vol. 39 No. 3, Fall 2008, 411–428.

vi) Thus it is respectfully submitted that while it may at the outset seem inherently harmless and innocuous to lay down the parameters of privacy, it may result in a limiting the role of citizen or the role of State in one way or the other if the privacy is to held to be fundamental right. As stated above, it is

---

[10]Dean William Prosser, "Privacy," *California Law Review* 48 (1960): 383, 389, quoted in E. Alderman and C. Kennedy, *The Right to Privacy* (New York: Alfred A. Knopf, 1995), 155–56.
[11]Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1968); Adam D. Moore, *Intellectual Property and Information Control* (New Brunswick, NJ: Transaction Publishing, 2001, 2004).
[12]*Eisenstadt v. Baird*, 405 U.S. 438 (1972): 453. See also Louis Henkin, "Privacy and Autonomy," *Columbia Law Review* 74 (1974): 1410, 1425; Joel Feinberg, "Autonomy, Sovereignty, and Privacy: Moral Ideas in the Constitution?" *Notre Dame Law Review* 58 (1983): 445; Daniel R. Ortiz, "Privacy, Autonomy, and Consent," *Harvard Journal of Law and Public Policy* 12 (1989): 91; and H. TristramEnglehardt Jr., "Privacy and Limited Democracy," *Social Philosophy and Policy* 17 (Summer 2000): 120–40.
[13]W. A. Parent, "Privacy, Morality, and the Law," *Philosophy and Public Affairs* 12 (1983): 269.
[14]Julie Inness, *Privacy, Intimacy, and Isolation* (New York: Oxford University Press, 1992)
[15]DeCew, *In Pursuit of Privacy*, 58, 64. DeCew

seen that for the better part of the century, foremost legal scholars have not been able to define the contours of privacy. It's been an almost unanimous view that any exercise to include such a concept within the fundamental rights framework may do violence to the delicate balance of state machinery and individual citizenry. The criticism of the American approach, highly relied upon by the Petitioner is perfectly conceptualised in an essay on the seminal work of Warren and Brandeis in the Harvard Law Review article in 1890. The professor Dorothy J. Glancy, in her article "The Invention Of The Right To Privacy", in Arizona Law Review, states that:

> "***Fewer than ninety years later it is surprising to find that this relatively new chapter in our law appears to have fallen into such disarray that one United States Supreme Court Justice has characterized the right to privacy cases decided by his Court as "defying categorical description".***
>
> ...
>
> *All that Warren and Brandeis ever claimed to have invented was a legal theory which brought into focus a common "right to privacy"* ***denominator already present in a wide variety of legal concepts*** *and precedents from many different areas of the common law. It is for that reason that their article reads as if the authors had literally ransacked every traditional area of the common law they could find-such as contracts, property, trusts, copyright, protection of trade secrets, and torts-in order to pluck out the already existing legal principle underlying all of these various parts of the common law. This underlying legal principle was the right to privacy."*

Dorothy J. Glancy, The Invention Of The Right To Privacy, Arizona Law Review, Volume 21 1979 Number 1

5. Thus it is clear from the above that not only "privacy" as a concept is incapable of being precisely defined but also its application on various facets of human behaviour and activities are essentially individual specific, therefore, incapable of any "judicially discernable and manageable standard" according to which it can be enforced. As such in absence of any precise guidance as to what conduct of human life is covered under the concept of "privacy" it cannot be conferred with a Constitutional status of a "protected fundamental right".

II. The codified statutory law in India already confers protection to individuals' 'Right to Privacy'.

6. It is respectfully submitted that as stated above, ascertaining the contours of the proposed right to privacy within the Constitutional setup could be a daunting task. Further, such right would have to stand the test of fast changing time wherein new avenues, technological advancements and fields are emerging rapidly.

In this changing scenario privacy can be best protected through statutory legislations which would be dealing with subject specific legislations which can precisely define the conduct and/or activity of humans requiring protection and also provide for breach thereof in absence of which only, a Constitutional remedy under Article 226 can be resorted to.

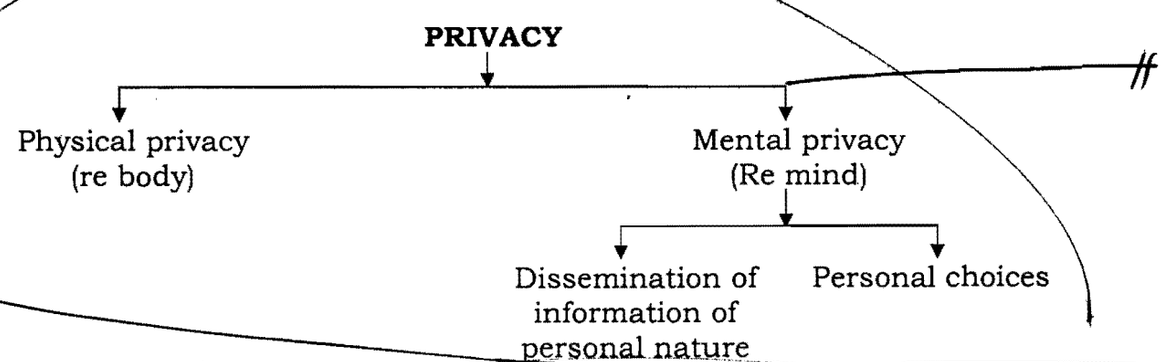
It is submitted that when a Statute is subject specific, it will not be difficult for the competent legislature to either define "privacy" or provide for its protections in the context of such a specific subject.

7. In this context, it is extremely crucial to note here that it is completely incorrect to suggest that the mandate of Article 12 of the Universal Declaration of Human Rights and Article 17 of International Covenant of Civil and Political Rights which provides for protection against arbitrary or unlawful interference with individual's privacy, family, home and correspondence, and which seeks to protect unlawful attacks on his honour and reputation has not been embodied in Indian law as submitted by some of the petitioners.

It is respectfully submitted that wherever, competent legislature has deemed it fit, expedient, desirable or necessary to protect privacy in any aspect of human life, the legislature has protected the same under a specific statue.

It is submitted that by enacting respective statutes dealing with specific subjects as detailed hereinafter, not only the legislature has protected individual's privacy in family, home, correspondence, and unlawful attacks on his honour and reputation but the legislature, in its wisdom, has also protected privacy in other facets of human life.

The question of protecting "privacy" as a "right" can be broadly classified as under:



The following are the broad facets of privacy. The list is obviously illustrative and not exhaustive:-

i. Physical privacy
ii. Privacy in one's home
iii. Privacy in Communication
iv. Privacy in Financial affairs
v. Privacy of Health
vi. Privacy of individual Information
vii. Online privacy
viii. Privacy of thought

8. It is respectfully submitted that wherever legislature deemed it fit and expedient, the above facets of "common law right of privacy" have been statutorily recognised, codified, defined and protected under the respective statutes, with a safeguard that the same cannot be abridged in any manner other than as provided under those specific statutes.

The same is evident from the following illustrative chart, which provides for laws which protect privacy of individuals in specific fields:-

[illegible] providing privacy in one's affairs, though [illegible]	
The Right To Information Act, 2005	**Section 8 (j)** of the Act forbids disclosure of information which relates to personal information the disclosure of which has not relationship to any public activity or interest, or **which would cause unwarranted invasion of the privacy of the individual** The test for disclosure of the said information under the Act is that the authority created under the has to be satisfied that the larger public interest justifies the disclosure of such information.
The Indian Easements Act, 1882	**Section 18** of the Act provides for Customary easement and provides that by the custom of a certain town no owner or occupier of a house can open a new window therein **so as substantially to invade his neighbour's privacy.**
Indian Penal Code, 1860	Indian penal code comprehensively covers almost all the aspect of human privacy including but not limiting to individual's privacy, family privacy, home and correspondence privacy, and protection against unlawful attacks on individuals honour and reputation. **Privacy of property** - 268. - Public nuisance "A person is guilty of a public nuisance who does any act or is guilty of an illegal omission which causes any common injury, danger or annoyance to the public

	or to the people in general who dwell or occupy property in the vicinity, or which must necessarily cause injury, obstruction, danger or annoyance to persons who may have occasion to use any public right." - Section 441 - Criminal trespass "Whoever enters into or upon property in the possession of another with intent to commit an offence or to intimidate, insult or annoy any person in possession of such property, or having lawfully entered into or upon such property, unlawfully remains there with intent thereby to intimidate, insult or annoy any such person, or with intent to commit an offence, is said to commit "criminal trespass"." - Section 442 - House trespass "Whoever commits criminal trespass by entering into or remaining in any building, tent or vessel used as a human dwelling. or any building used as a place for worship, or as a place for the custody of property, is said to commit "House-trespass"." - Section 443 - Lurking house-trespass "Whoever commits house-trespass having taken precautions to conceal such house-trespass from some person who has a right to exclude or eject the trespasser from the building, tent or vessel which is the subject of the trespass, is said to commit "lurking house-trespass"." - Section 444 - Lurking house-trespass by night "Whoever commits lurking house-trespass after sunset and before sunrise, is said to commit "lurking house-trespass by night"." - Section 445 - House breaking "A person is said to commit "house-breaking" who commits house-trespass if he effects his entrance into the house or any part of it in any of the six ways here in after described; or if, being in the house or any part of it for the purpose of

committing an offence, or, having committed an offence therein, he quits the house or any part of it in any of such six ways, that is to say:-

First- If he enters or quits through a passage by himself, or by any abettor of the house-trespass, in order to the committing of the house-trespass.

Secondly- If he enters or quits through any passage not intended by any person, other than himself or an abettor of the offence, for human entrance; or through any passage to which he has obtained access by scaling or climbing over any wall or building.

Thirdly- If lie enters or quits through any passage which he or any abettor of the house-trespass has opened, in order to the committing of the house-trespass by any means by which that passage was not intended by the occupier of the house to be opened.

Fourthly- If he enters or quits by opening any lock in order to the committing of the house-trespass, or in order to the quitting of the house after a house-trespass.

Fifthly- If he effects his entrance or departure by using criminal force or committing an assault or by threatening any person with assault.

Sixthly- If he enters or quits by any passage which he knows to have been fastened against such entrance or departure, and to have been unfastened by himself or by an abettor of the house-trespass."

- Section 446 - House-breaking by night

"Whoever commits house-breaking. after sunset and before sunrise, is said to commit "house- breaking by night"."

- Section 449 - House-trespass in order to commit offence punishable with death

"Whoever commits house-trespass in order to the committing of any offence punishable with death, shall be punishable with 152[imprisonment for life], or with rigorous imprisonment for a term not exceeding ten years, and shall also be liable to fine."

	- Section 450 - House-trespass in order to commit offence punishable with imprisonment for life "Whoever commits house-trespass in order to the committing of any offence punishable with [imprisonment for life], shall be punished with imprisonment of either description for a term not exceeding. ten years, and shall also be liable to fine." - Section 451 - House-trespass in order to commit offence punishable with imprisonment "Whoever commits house-trespass in order to the committing of any offence punishable with imprisonment, shall be punished with imprisonment of either description for a term which may extend to two years, and shall also be liable to fine; and if the offence intended to be committed is theft, the term of the imprisonment may be extended to seven years." - Section 452 - House-trespass after preparation for hurt, assault or wrongful restraint "Whoever commits house-trespass, having made preparation for causing hurt to any person or for assaulting any person, or for wrongfully restraining any person, or for putting any person in fear of hurt, or of assault, or of wrongful restraint, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine." - Section 458 - Lurking house-trespass or house-breaking by night after preparation for hurt, assault, or wrongful restraint - Section 459 - Grievous hurt caused whilst committing lurking house trespass or housebreaking - Section 461 - Dishonestly breaking open receptacle containing property

	- Section 462 - Punishment for same offence when committed by person entrusted with custody
Indian Evidence Act	- Section 122. Communications during marriage. No person who is or has been married, shall be compelled to disclose any communication made to him during marriage by any person to whom he is or has been married; nor shall he be permitted to disclose any such communication, unless the person who made it, or his representative in interest, consents, except in suits between married persons, or proceedings in which one married person is prosecuted for any crime committed against the other. - Section 124. Official communications No public officer shall be compelled to disclose communications made to him in official confidence, when he considers that the public interests would suffer by the disclosure. - Section 125. Information as to commission of offences No Magistrate or Police officer shall be compelled to say whence he got any information as to the commission of any offence, and no Revenue officer shall be compelled to say whence he got any information as to the commission of any offence against the public revenue.1[125. Information as to commission of offences.—No Magistrate or Police officer shall be compelled to say whence he got any information as to the commission of any offence, and no Revenue officer shall be compelled to say whence he got any information as to the commission of any offence against the public revenue." Explanation.—"Revenue officer" in this section means an officer employed in or about the business of any branch of the public revenue.] - Section 126 Professional communications No barrister, attorney, pleader or vakil shall at any time be permitted, unless with

	his client's express consent, to disclose any communication made to him in the course and for the purpose of his employment as such barrister, pleader, attorney or vakil, by or on behalf of his client, or to state the contents or condition of any document with which he has become acquainted in the course and for the purpose of his professional employment, or to disclose any advice given by him to his client in the course and for the purpose of such employment: Provided that nothing in this section shall protect from disclosure— (1) Any such communication made in furtherance of any [illegal] purpose; [illegal] purpose;" (2) Any fact observed by any barrister, pleader, attorney or vakil, in the course of his employment as such, showing that any crime or fraud has been committed since the commencement of his employment. It is immaterial whether the attention of such barrister, [pleader], attorney or vakil was or was not directed to such fact by or on behalf of his client. Explanation.—The obligation stated in this section continues after the employment has ceased. Illustrations (a) A, a client, says to B, an attorney—"I have committed forgery, and I wish you to defend me". As the defence of a man known to be guilty is not a criminal purpose, this communication is protected from disclosure. (b) A, a client, says to B, an attorney—"I wish to obtain possession of property by the use of a forged deed on which I request you to sue". This communication, being made in furtherance of a criminal purpose, is not protected from disclosure. (c) A, being charged with embezzlement, retains B, an attorney, to defend him. In the course of the proceedings, B observes that an entry has been made in A's account-book, charging A with the sum said to have been embezzled, which entry was not in the book at the commencement of his employment. This being a fact observed by B in the course of his employment, showing that a fraud has been committed since the commencement of the proceedings, it is not protected from

	disclosure. - Section 127 - Section 126 to apply to interpreters, etc The provisions of section 126 shall apply to interpreters, and the clerks or servants of barristers, pleaders, attorneys, and vakils. - Section 128 - Privilege not waived by volunteering evidence If any party to a suit gives evidence therein at his own instance or otherwise, he shall not be deemed to have consented thereby to such disclosure as is mentioned in section 126; and if any party to a suit or proceeding calls any such barrister, 1[pleader], attorney or vakil as a witness, he shall be deemed to have consented to such disclosure only if he questions such barrister, attorney or vakil on matters which, but for such question, he would not be at liberty to disclose.—If any party to a suit gives evidence therein at his own instance or otherwise, he shall not be deemed to have consented thereby to such disclosure as is mentioned in section 126; and if any party to a suit or proceeding calls any such barrister, 1[pleader], attorney or vakil as a witness, he shall be deemed to have consented to such disclosure only if he questions such barrister, attorney or vakil on matters which, but for such question, he would not be at liberty to disclose." - Section 129. Confidential communications with legal advisers No one shall be compelled to disclose to the Court any confidential communication which has taken place between him and his legal professional adviser, unless he offers himself as a witness, in which case he may be compelled to disclose any such communications as may appear to the Court necessary to be known in order to explain any evidence which he has given, but no others. - Section 130 - Production of title-deeds of witness not a party No witness who is not a party to a suit

	shall be compelled to produce his title-deeds to any property, or any document in virtue of which he holds any property as pledgee or mortgagee, or any document the production of which might tend to criminate him, unless he has agreed in writing to produce them with the person seeking the production of such deeds or some person through whom he claims. - Section 131 - Production of documents or electronic records which another person, having possession, could refuse to produce No one shall be compelled to produce documents in his possession or electronic records under his control, which any other person would be entitled to refuse to produce if they were in his possession, or control, unless such last-mentioned person consents to their production.]2[131. Production of documents or electronic records which another person, having possession, could refuse to produce.—No one shall be compelled to produce documents in his possession or electronic records under his control, which any other person would be entitled to refuse to produce if they were in his possession, or control, unless such last-mentioned person consents to their production.]"

Laws in India providing privacy in Communication	
Indian Telegraph Act, 1885	The Act contains several provisions which regulate and **prohibit the unauthorized interception or tampering with messages sent over 'telegraphs'**. **Section 5** of the Act empowers the Government to take possession of licensed telegraphs and to order interception of messages in cases of 'public emergency' or 'in the interest of the public safety'. Interception may only be carried out pursuant to a written order by an officer specifically empowered for this purpose by the State/Central Government. The officer must be 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" **Section 24** makes it a criminal offence for a person to enter a telegraph office "with the intent of unlawfully learning the contents of any message". Such a person may be punished with imprisonment for a term of up to a year. **Section 25** further imposes a criminal penalty on anyone who damages or tampers with any telegraph with the intent to prevent the transmission of messages or to acquaint himself with the contents of any message or to commit mischief. Punishment in this case could extend to 3 years imprisonment or a fine or both. **Section 26** makes it an offence for a Telegraph Officer to alter, unlawfully disclose or acquaint himself with the content of any message. This is also punishable with up to 3 years imprisonment or a fine or both. **Section 30** criminalizes the fraudulent retention or willful detention of a message which is intended for someone else. Punishment extends to 2 years imprisonment or fine or both.
License Agreements granted under the Telegraph Act	Although the statute itself governs the actions of telecom operators in a general way, more detailed guidelines protecting **individual privacy** regulating their behaviour are contained in the terms of the licenses issued to the telecoms which permit them to conduct businesses. Frequently, these licenses contain clauses requiring telecom operators to safeguard the privacy of their consumers. A few examples include: **Clause 21** of the National Long Distance License comprehensively covers various aspects of **privacy** including a. Licensees to be responsible for the protection of **privacy** of communication, and to ensure that unauthorised interception of message does not take place. b. Licensees to take all necessary steps to safeguard the **privacy** and **confidentiality** of any information about a third party and

	their business to whom they provide service and from whom they have acquired such information by virtue of those service and shall use their best endeavors to secure that: i. No person acting on behalf of the Licensees or the Licensees themselves divulge or uses any such information except as may be necessary in the course of providing such service to the Third Party; and ii. No such person seeks such information other than is necessary for the purpose of providing service to the Third Party. c. The above safeguard however does not apply where i. The information relates to a specific party and that party has consented in writing to such information being divulged or used, and such information is divulged or used in accordance with the terms of that consent; or ii. The information is already open to the public and otherwise known. d. The Licensees shall take necessary steps to ensure that the they and any person(s) acting on their behalf observe confidentiality of customer information. 2) **Clause 39.2** of the Unified Access Service License and clause 42.2 of the Cellular Mobile Telephone Service licence enjoin the licensee to take all necessary steps to safeguard the privacy and confidentiality of any information about a third party, and its business to whom it provides the service. The Licensee is required to use its best endeavors to secure that no person acting on behalf of the licensee or the licensee divulges or uses any such information - except as may be necessary in the course of providing such service to the third party. 3) The Internet Services License Agreement (which authorizes ISPs to function in India) similarly contains provisions touching on privacy: a) Part VI of the License Agreement gives the Government the right to inspect/monitor the TSPs systems. The TSP is responsible for making facilities available for such interception. b) **Clause 32** under Part VI contains

	provisions mandating the confidentiality of information. These provisions are identical to those described in Clause 21 of the NLD License agreement (see above). c) **Clause 33.4** makes it the responsibility of the TSP to trace nuisance, obnoxious or malicious calls, messages or communications transported through its equipment. d) **Clause 34.8** requires ISPs to maintain a log of all users connected and the service they are using (mail, telnet, http etc.). The ISPs must also log every outward login or telnet through their computers. These logs, as well as copies of all the packets originating from the Customer Premises Equipment (CPE) of the ISP, must be available in REAL TIME to Telecom Authority. The Clause forbids logins where the identity of the logged-in user is not known. e) **Clause 34.12** and **34.13** requires the Licensee to make available a list of all subscribers to its services on a password protected website for easy access by Government authorities. f) **Clause 34.16** requires the Licensee to activate services only after verifying the bonafides of the subscribers and collecting supporting documentation. There is no regulation governing how long this information is to be retained. g) **Clause 34.22** makes it mandatory for the Licensee to make available "details of the subscribers using the service" to the Government or its representatives "at any prescribed instant". h) **Clause 34.23** mandates that the Licensee maintain "all commercial records with regard to the communications exchanged on the network" for a period of "at least one year for scrutiny by the Licensor for security reasons and may be destroyed thereafter unless directed otherwise by the licensor". i) Clause 34.28 (viii) forbids the licensee from transferring the following information to any person/place outside India: j) Any accounting information relating to subscriber (except for international roaming/billing) (Note: it does not restrict a

	statutorily required disclosure of financial nature) ; and k) User information (except pertaining to foreign subscribers using Indian Operator's network while roaming). l) Clause 34.28(ix) and (x) require the TSP to provide traceable identity of their subscribers and on request by the Government must be able to provide the geographical location of any subscriber at any given time. m) Clause 34.28(xix) stipulates that "in order to maintain the privacy of voice and data, monitoring shall only be upon authorisation by the Union Home Secretary or Home Secretaries of the States/Union Territories". (It is unclear whether this is to operate as an overriding provision governing all other clauses as well)
Privacy and Confidentiality Direction by TRAI	Vide its 2010 directions TRAI has sought to implement the privacy and confidentiality related clauses in the service providers' licenses. Accordingly by this direction, the TRAI ordered all service providers to **"put in place an appropriate mechanisms, so as to prevent the breach of confidentiality on information belonging to the subscribers and privacy of communication"**. All service providers were required by this regulation to submit a report to the TRAI giving details of measures so adopted.

The Bankers Book Evidence Act, 1891	Acts confers statutory protections against inspection and dissemination of bankers books of accounts. Section 2A. Conditions in the printout. A printout of entry or a copy of printout referred to in sub-section (8) of section 2 shall be accompanied by the following, namely: (a) a certificate to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager; and (b) a certificate by a person in-charge of computer system containing a brief description of the computer system and the particulars of (A) the safeguards adopted by the system to ensure that data is entered or any other

	operation performed only by authorised persons; (B) the safeguards adopted to prevent and detect unauthorised change of data; (C) the safeguards available to retrieve data that is lost due to systemic failure or any other reasons; (D) the manner in which data is transferred from the system to removable media like floppies, discs, tapes or other electro-magnetic data storage devices; (E) the mode of verification in order to ensure that data has been accurately transferred to such removable media; (F) the mode of identification of such data storage devices; (G) the arrangements for the storage and custody of such storage devices; (H) the safeguards to prevent and detect any tampering with the system; and (I) any other factor which will vouch for the integrity and accuracy of the system. (c) a further certificate from the person in-charge of the computer system to the effect that to the best of his knowledge and belief, such computer system operated properly at the material time, he was provided with all the relevant data and the printout in question represents correctly, or is appropriately derived from, the relevant data. <u>Section 5. Case in which officer of bank not compellable to produce books</u> No officer of a bank shall in any legal proceeding to which the bank is not a party be compellable to produce any bankers book the contents of which can be proved under this Act, or to appear as a witness to prove the matters, transactions and accounts therein recorded, unless by order of the Court or a Judge made for special cause. <u>Section 6. Inspection of books by order of Court or Judge</u> (1) On the application of any party to a legal proceeding the Court or a Judge may order that such party be at liberty to inspect and take copies of any entries in a bankers book for any of the purposes of such proceeding, or may order the bank to prepare and produce, within a time to be specified in the order, certified copies of all such entries accompanied by a further certificate that no other entries are to be found in the books of the bank relevant to the matters in issue in such proceeding, and such further certificate shall be dated and subscribed in manner hereinbefore directed in reference to certified copies. (2) An order under this or the preceding section may be made either with or without summoning the bank, and shall be served on the bank three clear days (exclusive of bank holidays) before the

	same is to be obeyed, unless the Court or Judge shall otherwise direct. (3) The bank may at any time before the time limited for obedience to any such order as aforesaid either offer to produce their books at the trial or give notice of their intention to show cause against such order, and thereupon the same shall not be enforced without further order.
Credit Information Companies (Regulation) Act, 2005	Chapter VI of the Act embodies information privacy principles with respect to credit information Section 2 - Definitions.- e. "credit information company" means a company formed and registered under the Companies Act, 1956 and which has been granted a certificate of registration under sub-section (2) of section 5; f. "credit institution" means a banking company and includes- i. a corresponding new bank, the State Bank of India, a subsidiary bank, a co-operative bank, the National Bank and regional rural bank; ii. a non-banking financial company as defined under clause (f) of section 45-I of the Reserve Bank of India Act, 1934; l. "specified user" means any credit institution, credit information company being a member under sub-section (3) of section 15, and includes such other person or institution as may be specified by regulations made, from time to time, by the Reserve Bank for the purpose of obtaining credit information from a credit information company; Section 19 - Accuracy and security of credit information.-A credit information company or credit institution or specified user, as the case may be, in possession or control of credit information, shall take such steps (including security safeguards) as may be prescribed, to ensure that the data relating to the credit information maintained by them is accurate, complete, duly protected against any loss or unauthorised access or use or unauthorised disclosure thereof. Section 20. Privacy principles.- Every credit information company, credit institution and specified user, shall adopt the following privacy principles in relation to collection, processing, collating, recording, preservation, secrecy, sharing and usage of credit information, namely:- a. the principles- i. which may be followed by every

	credit institution for collection of information from its borrowers and clients and by every credit information company, for collection of information from its member credit institutions or credit information companies, for processing, recording, protecting the data relating to credit information furnished by, or obtained from, their member credit institutions or credit information companies, as the case may be, and sharing of such data with specified users; ii. which may be adopted by every specified user for processing, recording, preserving and protecting the data relating to credit information furnished, or received, as the case may be, by it; iii. which may be adopted by every credit information company for allowing access to records containing credit information of borrowers and clients and alteration of such records in case of need to do so; b. the purpose for which the credit information may be used, restriction on such use and disclosure thereof; c. the extent of obligation to check accuracy of credit information before furnishing of such information to credit information companies or credit institutions or specified users, as the case may be; d. preservation of credit information maintained by every credit information company, credit institution, and specified user as the case may be (including the period for which such information may be maintained, manner of deletion of such information and maintenance of records of credit information); e. networking of credit information companies, credit institutions and specified users through electronic mode; f. any other principles and procedures relating to credit information which the Reserve Bank may consider necessary and appropriate and may be specified by regulations. <u>Section 22. Unauthorised access to credit information.-</u> 1. No person shall have access to credit information in the possession or control of a credit information company or a credit institution or a specified user unless the access is authorised by this Act or any other law for the time being in force or directed to do so by any court or tribunal and any such access to credit information without such authorisation or direction shall be considered as an unauthorised access to credit information. 2. Any person who obtains unauthorised access to credit information as referred to in sub-section (1) shall be punishable with fine which may extend to one lakh rupees in respect of each offence and if he continues to have such

	unauthorised access, with further fine which may extend to ten thousand rupees for every day on which the default continues and such unauthorised credit information shall not be taken into account for any purpose. [The said Act also provides for penal provision for violation of privacy]
Public Financial Institutions (Obligation as to Fidelity and Secrecy) Act, 1983	The Act imposes a bar on public financial institutions to disclose information relating to affairs of its constituents Section 2. Definitions.— (1) In this Act, "public financial institution" means— (a) the Industrial Credit and Investment Corporation of India Limited, a company formed and registered under the Indian Companies Act, 1913 (7 of 1913); (b) the Industrial Reconstruction Corporation of India Limited, a company formed and registered under the Companies Act, 1956 (1 of 1956); or (c) any other institution, being a company as defined in section 617 of the Companies Act, 1956 (1 of 1956) or a company to which the provisions of section 619 of that Act apply, which the Central Government may, having regard to the nature of the business carried on by such institution, by notification in the Official Gazette, specify to be a public financial institution for the purposes of this Act. (2) Every notification issued under clause (c) of sub-section (1) shall, as soon as may be, after it is issued, be laid before each House of Parliament. Section 3. Obligation as to fidelity and secrecy.— (1) A public financial institution shall not, except as otherwise provided in sub-section (2) or in any other law for the time being in force, divulge any information relating to, or to the affairs of, its constituents except in circumstances in which it is, in accordance with the law or practice and usage, customary among bankers, necessary or appropriate for the public financial institution to divulge such information. (2) A public financial institution may, for the purpose of efficient discharge of its functions, collect from, or furnish to,— (a) the Central Government; or (b) the State Bank of India constituted under section 3 of the State Bank of India Act, 1955 (23 of 1955), any subsidiary bank within the meaning of the State Bank of India (Subsidiary Banks) Act, 1959 (38 of 1959), any corresponding new bank constituted under section 3 of the Banking Companies (Acquisition

	and Transfer of Undertakings) Act, 1970 (5 of 1970) or under section 3 of the Banking Companies (Acquisition and Transfer of Undertakings) Act, 1980 (40 of 1980), any other scheduled bank within the meaning of the Reserve Bank of India Act, 1934 (2 of 1934); or (c) any other public financial institution, such credit information or other information as it may consider useful for the purpose, in such manner and at such time as it may think fit. Explanation.—For the purposes of this sub-section, the expression "credit information" shall have the same meaning as in clause (c) of section 45A of the Reserve Bank of India Act, 1934 (2 of 1934) subject to the modification that the banking company referred to therein shall mean a bank referred to in clause (b) of this sub-section or a public financial institution. 1 [(3) Nothing contained in this section shall apply to the credit information disclosed under the Credit Information Companies (Regulation) Act, 2005.]
Payment and Settlement Systems Act, 2007	**Section 15** of the Act grants confidentiality to the document or information obtained by the Reserve Bank from the system provider which provides payment system for credit card, debit card related transactions [eg VISA] Section 15. Information, etc., to be confidential. – 1. Subject to the provisions of sub-section (2), any document or information obtained by the Reserve Bank under sections 12 to 14 (both inclusive) shall be kept confidential. 2. Notwithstanding anything contained in sub-section (1), the Reserve Bank may disclose any document or information obtained by it under sections 12 to 14 (both inclusive) to any person to whom the disclosure of such document or information is considered necessary for protecting the integrity, effectiveness or security of the payment system, or in the interest of banking or monetary policy or the operation of the payment systems generally or in the public interest.
Indian Income Tax Act, 1961	Act provides for confidentiality of income and tax information of the Assessee;
Fair Practice Code for Credit Card Operations, 2010	Under these guidelines banks/NBFCs are directed to **ensure confidentiality** of the customer's records and maintain fair practices in debt collection. The said guidelines also lays down that no bank or its agents would resort to **invasion of privacy** viz., persistently bothering the card holders/their family members at odd hours, either for offering of credit card or for the purpose of recovery of the balance amount. It also provides for violation of "do not call" code

	etc.
The Right To Information Act, 2005	**Section 8(d)** of the said provides exemption from disclosure of information if the said information contains commercial confidence, trade secrets or intellectual property and disclosure of which would harm the competitive position of a third party. The said information is disclosed only if competent authority is satisfied that larger public interest warrants the disclosure of such information;

Laws protecting Common Law right of Privacy of Individual Information	
The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016	**Chapter VI Protection of Information** **28. Security and confidentiality of information.** The Authority shall ensure the security of identity information and authentication records of individuals. Subject to the provisions of this Act, the Authority shall ensure confidentiality of identity information and authentication records of individuals. The Authority shall take all necessary measures to ensure that the information in the possession or control of the Authority, including information stored in the Central Identities Data Repository, is secured and protected against access, use or disclosure not permitted under this Act or regulations made thereunder, and against accidental or intentional destruction, loss or damage. Without prejudice to sub-sections (1) and (2), the Authority shall- adopt and implement appropriate technical and organisational security measures; ensure that the agencies, consultants, advisors or other persons appointed or engaged for performing any function of the Authority under this Act, have in place appropriate technical and organisational security measures for the information; and ensure that the agreements or arrangements entered into with such agencies, consultants, advisors or other persons, impose obligations equivalent to those imposed on the Authority under this Act, and require such agencies, consultants, advisors and other persons to act only on instructions from the Authority.

	Notwithstanding anything contained in any other law for the time being in force, and save as otherwise provided in this Act, the Authority or any of its officers or other employees or any agency that maintains the Central Identities Data Repository shall not, whether during his service or thereafter, reveal any information stored in the Central Identities Data Repository or authentication record to anyone: **29. Restriction on sharing information.** No core biometric information, collected or created under this Act, shall be- shared with anyone for any reason whatsoever; or used for any purpose other than generation of Aadhaar numbers and authentication under this Act. The identity information, other than core biometric information, collected or created under this Act may be shared only in accordance with the provisions of this Act and in such manner as may be specified by regulations. No identity information available with a requesting entity shall be- used for any purpose, other than that specified to the individual at the time of submitting any identity information for authentication; or disclosed further, except with the prior consent of the individual to whom such information relates. No Aadhaar number or core biometric information collected or created under this Act in respect of an Aadhaar number holder shall be published, displayed or posted publicly, except for the purposes as may be specified by regulations. **30. Biometric information deemed to be sensitive personal information.** The biometric information collected and stored in electronic form, in accordance with this Act and regulations made thereunder, shall be deemed to be "electronic record" and "sensitive personal data or information", and the provisions contained in the Information Technology Act, 2000 and the rules made thereunder shall apply to such information, in addition to, and to the extent not in derogation of the provisions of this Act. Explanation.- For the purposes of this section, the expressions-

	"electronic form" shall have the same meaning as assigned to it in clause (r) of sub-section (1) of section 2 of the Information Technology Act, 2000; "electronic record" shall have the same meaning as assigned to it in clause (t) of sub-section (1) of section 2 of the Information Technology Act, 2000; "sensitive personal data or information" shall have the same meaning as assigned to it in clause (iii) of the Explanation to section 43A of the Information Technology Act, 2000. **31. Alteration of demographic information or biometric information.** 1. In case any demographic information of an Aadhaar number holder is found incorrect or changes subsequently, the Aadhaar number holder shall request the Authority to alter such demographic information in his record in the Central Identities Data Repository in such manner as may be specified by regulations. 2. In case any biometric information of Aadhaar number holder is lost or changes subsequently for any reason, the Aadhaar number holder shall request the Authority to make necessary alteration in his record in the Central Identities Data Repository in such manner as may be specified by regulations. 3. On receipt of any request under sub-section (1) or sub-section (2), the Authority may, if it is satisfied, make such alteration as may be required in the record relating to such Aadhaar number holder and intimate such alteration to the concerned Aadhaar number holder. 4. No identity information in the Central Identities Data Repository shall be altered except in the manner provided in this Act or regulations made in this behalf. **32. Access to own information and records of requests for authentication.** The Authority shall maintain authentication records in such manner and for such period as may be specified by regulations. Every Aadhaar number holder shall be entitled to obtain his authentication record in such manner as may be specified by regulations. The Authority shall not, either by itself or through any entity under its control, collect, keep or maintain any information about the purpose of authentication.

	33. Disclosure of information in certain cases. 1. Nothing contained in sub-section (2) or sub-section (5) of section 28 or sub-section (2) of section 29 shall apply in respect of any disclosure of information, including identity information or authentication records, made pursuant to an order of a court not inferior to that of a District Judge: Provided that no order by the court under this sub-section shall be made without giving an opportunity of hearing to the Authority. 2. Nothing contained in sub-section (2) or sub-section (5) of section 28 and clause (b) of sub-section (1), sub-section (2) or sub-section (3) of section 29 shall apply in respect of any disclosure of information, including identity information or authentication records, made in the interest of national security in pursuance of a direction of an officer not below the rank of Joint Secretary to the Government of India specially authorised in this behalf by an order of the Central Government: Provided that every direction issued under this sub-section, shall be reviewed by an Oversight Committee consisting of the Cabinet Secretary and the Secretaries to the Government of India in the Department of Legal Affairs and the Department of Electronics and Information Technology, before it takes effect: Provided further that any direction issued under this sub-section shall be valid for a period of three months from the date of its issue, which may be extended for a further period of three months after the review by the Oversight Committee.
The Census Act, 1948	Protection from unauthorised disclosure of information gathered by the officers of state during the survey for census.
The Collection of Statistics Act, 2008	Protection from unauthorised disclosure of information furnished to the statistics officer or to any person or agencies authorised under the Act. Provision for keeping the identity of the informant confidential. [Chapter III - Section 9-14]
Justice (Care and Protection of Children) Act, 2000	Under **Section 3** of the Act the Central Government, the State Governments, the Board, and other agencies, as the case may be, while implementing the provisions of this Act are to be guided by principles of Principle of right to

	privacy and confidentiality. **Section 74** of the said Act prohibits disclosure of identity of children in any newspaper, magazine, news-sheet or audio-visual media or other forms of communication which may lead to the identification of a child in conflict with law or a child in need of care and protection or a child victim or witness of a crime. As per **Section 51** of the Act the report of the probation officer or social worker on a juvenile having been charged with the offence is be kept confidential;
The Protection of Children from Sexual Offences Act, 2012	Provides for protecting children's rights of privacy and confidentiality who are victim of offences of sexual assault, sexual harassment and pornography,

Laws protecting Online privacy	
The Information Technology Act, 2000	**Section 30** Certifying Authority to follow certain procedures Every Certifying Authority shall,- (a) make use of hardware, software, and procedures that the secure from intrusion and misuse; (b) provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions; (c) adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured; and (d) observe such other standards as may be specified by regulations. **Section 65** of the Act provides protection against tampering with individual's computer/ source documents. **Section 66** Hacking with Computer System. – (1) Whoever with the intent of cause or knowing that is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking. (2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both. **Section 66E** of the Act provides for punishment for violation of privacy. **Section 72** Breach of confidentiality and

	privacy.- Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.
Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011	India's most comprehensive data protection standards are found in the ITA and are known as the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011. The Rules seek to provide rights to the individual with regards to their information and obligate body corporate to take steps towards protecting the privacy of consumer's information. Among other things, the Rules define "sensitive personal information' and require that any corporate body must publish an online privacy policy, provide individuals with the right to access and correct their information, obtain consent before disclosing sensitive personal information ' except in the case of law enforcement, provide individuals the ability to withdraw consent, establish a grievance officer, require companies to ensure equivalent levels of protection when transferring information, and put in place reasonable security practices.

9. Thus, from the aforesaid illustrative statutory provisions it is clear that both pre and post independence, the legislature has been granting protection to the various facets and aspects of this "common law right to privacy" through statutes enacted by the competent legislatures. As such, in view thereof there is no justification to confer it a separate Constitutional protection under Part III of the Constitution by way of the process of judicial interpretation when it is impossible to lay down any definitive contours of the term "privacy".

III In other jurisdictions also "privacy" is protected by Statute

10. It is submitted that not only in India but in other jurisdictions also the there are instances where privacy is not conferred with a status of Constitutional right but the same has been protected under statutes governing various fields of human activity. This fact necessarily depends upon country specific parameters. The same is evident from the analysis of laws of the following countries which have codified the law relating to "individual privacy" which primarily defined as personal data and has granted in statutory safeguards from any state or private action:-

	PRIVACY LAW
NEW ZEALAND	**The Privacy Act 1993 ('Act')** governs how agencies collect, use, disclose, store, retain and give access to personal information. The Act gives the Privacy Commissioner the power to issue codes of practice that modify the operation of the Act in relation to specific industries, agencies, activities or types of personal information. Codes currently in place are: ➢ Credit Reporting Privacy Code ➢ Health Information Privacy Code ➢ Justice Sector Unique Identifier Code ➢ Superannuation Schemes Unique Identifier Code ➢ Telecommunications Information Privacy Code ➢ Civil Defence National Emergencies (Information Sharing) Code. Enforcement is through the Privacy Commissioner.
AUSTRALIA	Data privacy/protection in Australia is currently made up of a mix of Federal and State/Territory legislation. **The Federal Privacy Act 1988 (Cth) (Privacy Act) and its Australian Privacy Principles (APPs)** apply to private sector entities with an annual turnover of at least A$3 million and all Commonwealth Government and Australian Capital Territory Government agencies. The Privacy Act was last amended by the Privacy Amendment (Enhancing Privacy Protection) Act 2012, which came in to force on 12 March 2014. The amendments significantly strengthened the powers of the Privacy Commissioner to conduct investigations (including own motion investigations), ensure

	compliance with the amended Privacy Act and, for the first time, introduced civil penalties for a serious/egregious breach or for repeated breaches of the APPs where remediation has not been implemented.
ISRAEL	The laws that govern the right to privacy in Israel are the Basic Law: **Human Dignity and Liberty, 5752 - 1992; the Protection of Privacy Law, 5741-1981** and the regulations promulgated thereunder (the 'PPL') and the guidelines of ILITA (as defined below). The Israeli Law, Information and Technology Authority ("ILITA"), established in September 2006, as determined by Israel's Government decision no. 4660, dated 19.01.2006.
JAPAN	**The Act on the Protection of Personal Information ("APPI")** requires business operators who utilize for their business in Japan a personal information database which consists of more than 5,000 individuals in total identified by personal information on any day in the past six months to protect personal information. Amendments to the APPI, which were passed in 2015 and go into effect no later than September 2017[1] (the "Amendments"), apply the APPI to all businesses in Japan, regardless of whether the business operator maintains a database of more than 5,000 individuals. Further, the Amendments clarify the definition of personal information, add two new classes of information, and introduce new requirements for "opt out" choice for business operators to disclosure personal information to third parties. Finally, as of January 1, 2016, the Amendments created a Privacy Protection Commission (the "Commission"), a central agency which will Act as a supervisory governmental organization on issues of privacy protection. The Amendments created the Privacy Protection Commission (the "Commission"), which will Act as a supervisory governmental organization on issues of privacy protection.
CHINA	Currently, there is not a comprehensive data protection law in the People's Republic of China ('PRC'). Instead, rules relating to personal data protection are found across various laws and regulations. Generally speaking, provisions found in laws such as the General Principles of Civil Law and the Tort Liability Law may be used to interpret data protection rights as a right of reputation or right of privacy. However, such interpretation is not explicit. A draft Personal Data

	Protection Law has been under review by the PRC Government for many years, but there is still no indication as to if and when such law will be passed.
BRAZIL	Currently, Brazil does not have a single statute establishing data protection framework. There are two bills of laws, namely, No. 330/2013 and No. 5.276/2016, under analysis before Congress that, when enacted, will specifically and broadly regulate such subject matter locally. According to the developments of both future regulations, Bill of Law No. 5.2726/16 ("Bill of Law"), dated of May 13, 2016, is likely to be enacted in the near future, since the Presidency declared it with a status of urgency under the terms of Section 64 of Brazilian Federal Constitution, thus, Bill of Law No. 330/13 should be disregarded. In the absence of specific law, Federal Law No. 12.965/2014 ("Brazilian Internet Act"), and its recently enacted regulating Decree No. 8.771/16 ("Decree"), dated of May 11, 2016, has brought some provisions on security and processing of personal data.
SAUDI ARABIA	Shari'a principles (that is, Islamic principles derived from the Holy Quran and the Sunnah, the latter being the witnesses' sayings of the Prophet Mohammed), which although not codified, are the primary source of law in the KSA. In addition to Shari'a principles, the law in the KSA consists of secular regulations passed by government, which is secondary if it conflicts with Shari'a principles. At this time, there is no specific data protection legislation in place in the KSA (although we understand that a new freedom of information and protection of private data law is under review by the Shura Council). Shari'a principles generally protect the privacy and personal data of individuals.
QATAR	On 3 November 2016 the Qatari government passed a data protection law, Law No. (13) of 2016 Concerning Personal Data Protection ('Data Protection Law'). The Data Protection Law will come into effect within six months of the date of issue, that is 3 May 2017 (unless this period is extended). Qatar is the first GCC member state to issue a generally applicable data protection law. The Data Protection Law envisages further regulations being issued to assist its implementation. The Data Protection Law will apply to personal data when this data is processed electronically, or obtained, collected or extracted in any other way in preparation for the electronic processing thereof, or that is

	processed by combining electronic processing and traditional processing.
SINGAPORE	Singapore enacted the Personal Data Protection Act 2012 (No. 26 of 2012) ('Act') on 15 October 2012. The Act took effect in 3 phases: ➢ Provisions relating to the formation of the Personal Data Protection Commission (the 'Commission') took effect on 2 January 2013. ➢ Provisions relating to the National Do-Not-Call Registry ('DNC Registry') took effect on 2 January 2014. ➢ The main data protection provisions took effect on 2 July 2014. The Act has extraterritorial effect, and so applies to organisations collecting personal data from individuals in Singapore whether or not the organisation itself has a presence in Singapore. The data protection obligations under the Act do not apply to the public sector, to whom separate rules apply.
TAIWAN	The former Computer Processed Personal Data Protection Law ('CPPL') was renamed as the Personal Data Protection Law ('PDPL') and amended on 26 May 2010. The PDPL became effective on 1 October 2012, except that the provisions relating to sensitive personal data and the notification obligation for personal data indirectly collected before the effectiveness of the PDPL remained ineffective. The government later proposed further amendment to these and other provisions, which passed legislative procedure and became effective on 15th March 2016. In Taiwan, there is no single national data protection authority. The various ministries and city/county governments serve as the competent authorities. There is no requirement in Taiwan for the data controller to appoint a data protection officer. However, if the data controller is a government agency, a specific person should be appointed to be in charge of the security maintenance measures.
MALAYSIA	Malaysia's first comprehensive personal data protection legislation, the Personal Data Protection Act 2010 (PDPA), was passed by the Malaysian Parliament on 2 June 2010 and came into force on 15 November 2013. Pursuant to the PDPA, a Personal Data Protection Commissioner (Commissioner) has been appointed to implement the PDPA's provisions. Decisions of the Commissioner can be appealed against through the Personal Data Protection Appeal

	Tribunal.
MEXICO	The Federal Law on the Protection of Personal Data held by Private Parties (Ley Federal de Protección de DatosPersonalesenPosesión de losParticulares) (the 'Law') was enacted on July 5, 2010 and entered into force on July 6, 2010. The Executive Branch has also issued: ➢ the Regulations to the Federal Law on the Protection of Personal Data held by Private Parties (Reglamento de la Ley Federal de Protección de DatosPersonalesenPosesión de losParticulares) on December 21, 2011 (the 'Regulations'), same which entered into force on December 22, 2011. ➢ the Privacy Notice Guidelines on January 17, 2013 (the 'Guidelines') which entered into force on April 18, 2013. ➢ the Parameters for Self Regulation regarding personal data on May 29, 2014 (the 'Parameters'), which entered into force on May 30, 2014.
NIGERIA	Nigeria does not have a comprehensive legislative framework on the protection of personal data. However, there are a few industry-specific and targeted laws and regulations that provide some privacy-related protections, which include: ➢ The Constitution of the Federal Republic of Nigeria, 1999 (As Amended) ('the Constitution') which provides for the fundamental rights of its citizens and upholds the right of privacy as sacrosanct. Section 37 thereof provides for the guarantee and protection of the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications. ➢ The Freedom of Information Act, 2011 ('FOI Act') which seeks to protect personal privacy. Section 14 of the FOI Act provides that a public institution is obliged to deny an application for information that contains personal information unless the individual involved consents to the disclosure, or where such information is publicly available. Also, Section 16 of the FOI Act provides that a public institution may deny an application for disclosure of information that is subject to various forms of professional privilege conferred by law (such as lawyer-client privilege, health workers-client privilege, etc).

	➢ The Child Rights Act No. 26 of 2003 (the 'Child Rights Act') regulates the protection of children (persons under the age of 18 years). This Act limits access to information relating to children in certain circumstances. ➢ The Consumer Code of Practice Regulations 2007 ('the NCC Regulations') issued by the regulator of the telecommunications industry in Nigeria, the Nigerian Communications Commission ('NCC'). The NCC Regulations provide that all licensees must take reasonable steps to protect customer information against improper or accidental disclosure, and must ensure that such information is securely stored and not kept longer than necessary. It also provides that customer information must not be transferred to any party except to the extent agreed with the Customer, as permitted or required by the NCC or other applicable laws or regulations. ➢ In 2011, the NCC issued the Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations, 2011. Section 9 of the Regulation provides that subscribers information contained in the Central Database shall be held in strict confidentiality basis and no person or entity shall be allowed access to any subscriber's information that is on the Central Database except as prescribed by the Regulation. "Central Database" is defined in the Regulation to mean subscriber information database, containing the biometric and other registration information of all Subscribers . Section 21 of the Regulation provides penal sanctions for violators. ➢ The National Information Technology Development Agency ('NITDA') which is the national authority responsible for planning, developing and promoting the use of information technology in Nigeria, and which issues the Guidelines on Data Protection ('NITDA Guidelines') pursuant to the NITDA Act 2007. The NITDA Guidelines prescribe guidelines for organisations that obtain and process personal of Nigeria residents and citizens within and outside Nigeria for protecting such personal data. The NITDA Guidelines apply to federal,

	state and local government agencies and institutions as well as private sector organisations that own, use or deploy information systems within the Federal Republic of Nigeria.
PERU	Personal data protection is governed in Peru by: ➢ the Personal Data Protection Law No. 29733 ('PDPL') published on July 3, 2011 ➢ its regulations enacted by Supreme Decree 003-2013-JUS and published on March 22, 2013 (the 'Regulations'), and ➢ the Security Policy on Information Managed by Databanks of Personal Data enacted by Directorial Resolution N° 019-2013-JUS/DGPDP on October 11, 2013. Although several provisions of the PDPL have been in force since July 4, 2011, most of the provisions of the PDPL only came into force on May 8, 2013 (30 business days after the issuance of the Regulations).
SOUTH KOREA	In the past, South Korea did not have a comprehensive law governing data privacy. However, a law relating to protection of personal information (Personal Information Protection Act, 'PIPA') was enacted and became effective as of 30 September 2011. Moreover, there is sector specific legislation such as: ➢ the Act on Promotion of Information and Communication Network Utilisation and Information Protection ('IT Network Act') which regulates the collection and use of personal information by IT Service Providers, defined as telecommunications business operators under Article 2.8 of the Telecommunications Business Act; and other persons who provide information or intermediate the provision of information for profit by utilising services rendered by a telecommunications business operator ➢ the Use and Protection of Credit Information Act ('UPCIA') which regulates the use and disclosure of Personal Credit Information, defined as credit information which is necessary to determine the credit rating, credit transaction capacity, etc. of an individual person. The UPCIA primarily applies to Credit Information Providers/Users, defined under Article 2.7 of the UPCIA as a person (entity) prescribed by Presidential Decree

	thereof who provides any third party with credit information obtained or produced in relation to his/her own business for purposes of commercial transactions, such as financial transactions with customers, or who has been continuously supplied with credit information from any third party to use such information for his/her own business, and ➢ the Act on Real Name Financial Transactions and Guarantee of Secrecy ('ARNFTGS') which applies to information obtained by financial or financial services institutions. Under PIPA, except as otherwise provided for in any other Act, the protection of personal information shall be governed by the provisions of PIPA.
TRINIDAD & TOBAGO	In Trinidad and Tobago The Data Protection Act, 2011 provides for the protection of personal privacy and information ('DPA') processed and collected by public bodies and private organisations. The DPA was partially proclaimed on the 6th January 2012 by Legal Notice 2 of 2012 and only Part I and sections 7 to 18, 22, 23, 25(1), 26 and 28 of Part II have come into operation. No timetable has been set for the proclamation of the remainder of the DPA and it is possible that there may be changes to the remainder of the legislation before it is proclaimed.
UKRAINE	The Law of Ukraine No. 2297 VI 'On Personal Data Protection' as of 1 June 2010 (Data Protection Law) is the main legislative Act regulating relations in the sphere of personal data protection in Ukraine. At 20 December 2012 Data Protection Law has been substantially amended by the Law of Ukraine 'On introducing amendments to the Law of Ukraine "On personal data protection' dated 20 November 2012 No. 5491-VI. Additional significant changes to Data Protection Law were envisaged by the Law of Ukraine 'On Amendments to Certain Laws of Ukraine regarding Improvement of Personal Data Protection System' dated 3 July 2013 No. 383-VII which came into force on 1 January 2014. In addition to the Data Protection Law, certain data protection issues are regulated by subordinate legislation specifically developed to implement the Data Protection Law.

11. Thus, from the aforesaid analysis, it is clear that there are other jurisdiction in the world where no Constitutional protection is conferred to "right of privacy" nonetheless the same has been conferred statutory protection under respective statutes.

IV. Position under English Law Post their joining European Union

12. So far as right to privacy in England is concerned, it is treated merely as a common law right.

In examining the nature of the English cause of action for tort, it is necessary first of all to outline the distinctive nature of Article 8 ECHR rights.[16] The Article 8 right to a private life is a qualified right. Paragraph 2 provides that:

> *"1 Everyone has the right to respect for his private and family life, his home and his correspondence.*
> *2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

By its very nature, therefore, Art 8 envisages a balancing of competing rights, none of which is predominant, in determining whether the interference with Article 8 is lawful and a necessary or proportionate response. It has also been found to create negative and positive obligations on the State, to abstain from arbitrary interference in private or family life, but also to adopt measures designed to secure respect for private life even in private disputes.[17] While the State has a margin of appreciation in choosing the means by which to secure compliance with Article 8,[18] the nature of the State's obligation will depend on the particular aspect of private life that is at issue.[19] A wide margin of appreciation will exist in cases where the State is required to strike a balance between competing private and public interests or rights set out in the Convention for the Protection of Human Rights and

---

[16] See generally David Harris et al, Harris, O'Boyle, and Warbrick: Law of the European Convention on Human Rights (Oxford: Oxford University Press, 3rd Ed, 2014) ch 12.
[17] X and Y v The Netherlands (8978/80) (1986) 8 EHRR 235 at [23].
[18] See Handyside v UK (A/24) (1979–1980) 1 EHRR 737.
[19] Söderman v Sweden (5786/08) (2014) 58 EHRR 36. See also X and Y v the Netherlands (8978/80) (1986) 8 EHRR 235 at [24]; Von Hannover v Germany (No 2) (40660/08) (2012) 55 EHRR 15 at [104].

Fundamental Freedoms[20], although the court has indicated that where the interference involves a most intimate aspect of private life, the margin allowed to the State will be narrowed[21]. This position does signify, however, that there remains a lack of clarity as to the nature and extent of the positive obligations imposed by Article 8.[22]

13. This becomes clear from the following analysis of the decision rendered by House of Lords in the case of ***Wainwright Vs. Home Office*** reported in ***(2003) 3 WLR 1137***, which makes out following two points:-

a) That the even the apex court in England has refused to do is to formulate a general principle of "invasion of privacy" on Constitutional touchstone;

b) The concept of privacy is so inherently vague that even judicially trained minds can come to diametrically opposite conclusions on the same set of facts;

14. In this context it would be relevant to first analyse the said judgment from point (b) above.

a. In this case the court of first instance ie Leeds County Court held that the searches were wrongful (and hence not protected by authority of law) because of the battery and invasion of the Wainwrights' "right to privacy", which he conceived to be a trespass to the person. The court of first instance awarded Alan Wainwright £3,500 basic and £1,000 aggravated damages, and Mrs Wainwright £1,600 basic and £1,000 aggravated damages.

---

[20] (Eur TS No 5; 213 UNTS 221; 1953 UKTS No 71) (4 November 1950; entry into force 3 September 1953) (Evans v UK (6339/05) (2008) 46 EHRR 34)
[21] Söderman v Sweden (5786/08) (2014) 58 EHRR 36 at [79]
[22] David Harris et al, Harris, O'Boyle, and Warbrick: Law of the European Convention on Human Rights (Oxford: Oxford University Press, 3rd Ed, 2014) at p 533.

b. The Court of Appeal did not agree with the above judgment.

c. **The plaintiffs appealed to the House of Lords. Lord Hoffmann held that there was no tort for invasion of privacy, because (based on experience in the United States) it was too uncertain**. Moreover, a claim under Article 8 of the European Convention on Human Rights(ECHR), (right to privacy and family life), did not help because the ECHR was merely a standard which applied to whatever was currently present in the common law. Common law protection was sufficient privacy protection for the ECHR's purpose.

Thus from the above it is clear that on the same set of facts, even judicially trained minds have also come to diametrically opposite conclusions, while dealing with the case of personal privacy that it makes it obvious that expressions "privacy is so vague that there is no manageable standard by which a person can be said to have committed breach or not to have committed a breach of the said vague concept..

15. Furthermore it is also clear that the **apex court in England in the said case of Wainwright [Supra] refused to confer general principle of "invasion of privacy" a Constitutional status**. The same is clear from the following extract of the case which reproduced hereinbelow for ready reference:-

> ***"15** My Lords, let us first consider the proposed tort of invasion of privacy. Since the famous article by Warren and Brandeis ("The Right to Privacy" (1890) 4 Harvard LR 193) the question of whether such a tort exists, or should exist, has been much debated in common law jurisdictions. Warren and Brandeis suggested that one could generalise certain cases on defamation, breach of copyright in unpublished letters, trade secrets and breach of confidence as all based upon the protection of a common value which they called privacy or, following Judge Cooley (Cooley on Torts , 2nd ed (1888), p 29) "the right to be let alone". They said that identifying this common element should enable the courts to declare the existence of a general principle which protected a person's*

appearance, sayings, acts and personal relations from being exposed in public.

16 *Courts in the United States were receptive to this proposal and a jurisprudence of privacy began to develop. It became apparent, however, that the developments could not be contained within a single principle; not, at any rate, one with greater explanatory power than the proposition that it was based upon the protection of a value which could be described as privacy. Dean Prosser, in his work on The Law of Torts, 4th ed (1971), p 804, said that:*

> *"What has emerged is no very simple matter ... it is not one tort, but a complex of four. To date the law of privacy comprises four distinct kinds of invasion of four different interests of the plaintiff, which are tied together by the common name, but otherwise have almost nothing in common except that each represents an interference with the right of the plaintiff 'to be let alone'."*

17 *Dean Prosser's taxonomy divided the subject into* ***(1)*** *intrusion upon the plaintiff's physical solitude or seclusion (including unlawful searches, telephone tapping, long-distance photography and telephone harassment)* ***(2)*** *public disclosure of private facts and* ***(3)*** *publicity putting the plaintiff in a false light and* ***(4)*** *appropriation, for the defendant's advantage, of the plaintiff's name or likeness. These, he said, at p 814, had different elements and were subject to different defences.*

18 *The need in the United States to break down the concept of "invasion of privacy" into a number of loosely-linked torts must cast doubt upon the value of any high-level generalisation which can perform a useful function in enabling one to deduce the rule to be applied in a concrete case. English law has so far been unwilling, perhaps unable, to formulate any such high-level principle.* ***There are a number of common law and statutory remedies of which it may be said that one at least of the underlying values they protect is a right of privacy.*** *Sir Brian Neill's well known article "Privacy: a challenge for the next century" in Protecting Privacy (ed B Markesinis, 1999) contains a survey. Common law torts include trespass, nuisance, defamation and malicious falsehood; there is the equitable action for breach of confidence and statutory remedies under the Protection from Harassment Act 1997 and the Data Protection Act 1998. There are also extra-legal remedies under Codes of Practice applicable to broadcasters and newspapers.* ***But there are gaps; cases in which the courts have considered that an invasion of privacy deserves a remedy which the existing law does not offer. Sometimes the perceived gap can be filled by judicious development of an existing principle.*** *The law of breach of confidence has in recent years undergone such a process: see in particular the judgment of Lord Phillips of Worth Matravers MR in Campbell v MGN Ltd [2003] QB 633. On the other hand, an attempt to create a tort of telephone harassment by a radical change in the basis of the action for private nuisance in Khorasandjian v Bush [1993] QB 727 was held by the House of Lords in Hunter v Canary Wharf Ltd [1997] AC 655 to be a step too far.* ***The gap was filled by the 1997 Act.***

19 What the courts have so far refused to do is to formulate a general principle of "invasion of privacy" *(I use the quotation marks to signify doubt about what in such a context the expression would mean) from which the conditions of liability in the particular case can be deduced. The reasons were discussed by Sir Robert Megarry V-C in Malone v Metropolitan Police Comr [1979] Ch 344, 372–381. I shall be sparing in citation but the whole of Sir Robert's treatment of the subject deserves careful reading. The question was whether the plaintiff had a cause of action for having his telephone tapped by the police without any trespass upon his land. This was (as the European Court of Justice subsequently held in Malone v United Kingdom (1984) 7 EHRR 14) an infringement by a public authority of his right to privacy under article 8 of the Convention, but because there had been no trespass, it gave rise to no identifiable cause of action in English law. Sir Robert was invited to declare that invasion of privacy, at any rate in respect of telephone conversations, was in itself a cause of action. He said, at p 372:*

> *"I am not unduly troubled by the absence of English authority: there has to be a first time for everything, and if the principles of English law, and not least analogies from the existing rules, together with the requirements of justice and common sense, pointed firmly to such a right existing, then I think the court should not be deterred from recognising the right. On the other hand, it is no function of the courts to legislate in a new field. The extension of the existing laws and principles is one thing, the creation of an altogether new right is another."*

22 Once again, Parliament provided a remedy, subject to a detailed code of exceptions, in the Interception of Communications Act 1985. *A similar problem arose in R v Khan (Sultan) [1997] AC 558, in which the defendant in criminal proceedings complained that the police had invaded his privacy by using a listening device fixed to the outside of a house.* ***There was some discussion of whether the law should recognise a right to privacy which had been prima facie infringed, but no concluded view was expressed because all their Lordships thought that any such right must be subject to exceptions, particularly in connection with the detection of crime, and that the accused's privacy had been sufficiently taken into account by the judge when he exercised his discretion under section 78 of the Police and Criminal Evidence Act 1984 to admit the evidence obtained by the device at the criminal trial.*** *The European Court of Human Rights subsequently held (Khan v United Kingdom The Times, 23 May 2000) that the invasion of privacy could not be justified under article 8 because, in the absence of any statutory regulation, the actions of the police had not been "in accordance with law".* ***By that time, however, Parliament had intervened in the Police Act 1997 to put the use of surveillance devices on a statutory basis.***

26 All three judgments are flat against a judicial power to declare the existence of a high-level right to privacy and I do not think that they suggest that the courts should do so. *The members of the Court of Appeal certainly thought that it would be desirable if there was legislation to confer a right to protect the privacy of a person in the*

position of Mr Kaye against the kind of intrusion which he suffered, but they did not advocate any wider principle. And when the Calcutt Committee reported in June 1990, they did indeed recommend that "entering private property, without the consent of the lawful occupant, with intent to obtain personal information with a view to its publication" should be made a criminal offence: see the Report of the Committee on Privacy and Related Matters (1990) (Cm 1102), para 6.33. The Committee also recommended that certain other forms of intrusion, like the use of surveillance devices on private property and long-distance photography and sound recording, should be made offences.

27 But the Calcutt Committee did not recommend, even within their terms of reference (which were confined to press intrusion) the creation of a generalised tort of infringement of privacy: *paragraph 12.5. This was not because they thought that the definitional problems were insuperable. They said that if one confined the tort to "publication of personal information to the world at large" (paragraph 12.12) it should be possible to produce an adequate definition and they made some suggestions about how such a statutory tort might be defined and what the defences should be. But they considered that the problem could be tackled more effectively by a combination of the more sharply-focused remedies which they recommended: paragraph 12.32. As for a "general wrong of infringement of privacy", they accepted, at paragraph 12.12, that it would, even in statutory form, give rise to "an unacceptable degree of uncertainty". There is nothing in the opinions of the judges in Kaye v Robertson [1991] FSR 62 which suggests that the members of the court would have held any view, one way or the other, about a general tort of privacy.*

31 There seems to me a great difference between identifying privacy as a value which underlies the existence of a rule of law (and may point the direction in which the law should develop) and privacy as a principle of law in itself. ***The English common law is familiar with the notion of underlying values-principles only in the broadest sense-which direct its development.*** *A famous example is Derbyshire County Council v Times Newspapers Ltd [1993] AC 534, in which freedom of speech was the underlying value which supported the decision to lay down the specific rule that a local authority could not sue for libel. But no one has suggested that freedom of speech is in itself a legal principle which is capable of sufficient definition to enable one to deduce specific rules to be applied in concrete cases. That is not the way the common law works.*

32 Nor is there anything in the jurisprudence of the European Court of Human Rights which suggests that the adoption of some high level principle of privacy is necessary to comply with article 8 of the Convention. The European Court is concerned only with whether English law provides an adequate remedy in a specific case in which it considers that there has been an invasion of privacy contrary to article 8(1) and not justifiable under article 8(2). So in Earl Spencer v United Kingdom 25 EHRR CD 105 it was satisfied that the action for breach of confidence provided an adequate remedy for the Spencers' complaint and looked no further into the rest of the armoury of remedies available to the victims of other invasions of privacy. Likewise, in Peck v United Kingdom (2003) 36

EHRR 719 the court expressed some impatience, at paragraph 103, at being given a tour d'horizon of the remedies provided and to be provided by English law to deal with every imaginable kind of invasion of privacy. It was concerned with whether Mr Peck (who had been filmed in embarrassing circumstances by a CCTV camera) had an adequate remedy when the film was widely published by the media. It came to the conclusion that he did not.

***34** Furthermore, the coming into force of the Human Rights Act 1998 weakens the argument for saying that a general tort of invasion of privacy is needed to fill gaps in the existing remedies. Sections 6 and 7 of the Act are in themselves substantial gap fillers; if it is indeed the case that a person's rights under article 8 have been infringed by a public authority, he will have a statutory remedy. The creation of a general tort will, as Buxton LJ pointed out in the Court of Appeal [2002] QB 1334, 1360, para 92, pre-empt the controversial question of the extent, if any, to which the Convention requires the state to provide remedies for invasions of privacy by persons who are not public authorities.*

35 For these reasons I would reject the invitation to declare that since at the latest 1950 there has been a previously unknown tort of invasion of privacy."

16. Thus from the aforesaid it is clear that this concept "privacy" is so vague that it cannot be, in the present form, be declared a Fundamental Right as there are no judicially manageable standard to constitutionally enforce the same. The said right of privacy is sufficiently protected by appropriate statutes [as explained hereunder] depending upon the subject-specific precise and definable need for protection of privacy.

17. Further, following *Wainwright Vs. Home Office* reported in *(2003) 3 WLR 1137*, in **Campbell vs. MGN Limited** [2004] UKHL 22, the Court held:

11. **In this country, unlike the United States of America, there is no over-arching, all-embracing cause of action for 'invasion of privacy'**: see *Wainwright v Home Office* [2003] 3 WLR 1137. But protection of various aspects of privacy is a fast developing area of the law, here and in some other common law jurisdictions. The recent decision of the Court of Appeal of New Zealand in *Hosking v Runting* (25 March 2004) is an example of this. In this country development of the law has been spurred by enactment of the Human Rights Act 1998.

12. The present case concerns one aspect of invasion of privacy: wrongful disclosure of private information. The case

involves the familiar competition between freedom of expression and respect for an individual's privacy. Both are vitally important rights. Neither has precedence over the other. The importance of freedom of expression has been stressed often and eloquently, the importance of privacy less so. But it, too, lies at the heart of liberty in a modern state. A proper degree of privacy is essential for the well-being and development of an individual. And restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state: see La Forest J in *R v Dymont* [1988] 2 SCR 417, 426.

13. The common law or, more precisely, courts of equity have long afforded protection to the wrongful use of private information by means of the cause of action which became known as breach of confidence. A breach of confidence was restrained as a form of unconscionable conduct, akin to a breach of trust. Today this nomenclature is misleading. The breach of confidence label harks back to the time when the cause of action was based on improper use of information disclosed by one person to another in confidence. To attract protection the information had to be of a confidential nature. But the gist of the cause of action was that information of this character had been disclosed by one person to another in circumstances 'importing an obligation of confidence' even though no contract of non-disclosure existed: see the classic exposition by Megarry J in *Coco v A N Clark (Engineers) Ltd* [1969] RPC 41, 47-48. The confidence referred to in the phrase 'breach of confidence' was the confidence arising out of a confidential relationship.

14. This cause of action has now firmly shaken off the limiting constraint of the need for an initial confidential relationship. In doing so it has changed its nature. In this country this development was recognised clearly in the judgment of Lord Goff of Chieveley in *Attorney-General v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109, 281. **Now the law imposes a 'duty of confidence' whenever a person receives information he knows or ought to know is fairly and reasonably to be regarded as confidential**. Even this formulation is awkward. The continuing use of the phrase 'duty of confidence' and the description of the information as 'confidential' is not altogether comfortable. Information about an individual's private life would not, in ordinary usage, be called 'confidential'. The more natural description today is that such information is private. The essence of the tort is better encapsulated now as misuse of private information.

15. In the case of individuals this tort, however labelled, affords respect for one aspect of an individual's privacy. That is the value underlying this cause of action. An individual's privacy can be invaded in ways not involving publication of information. Strip-searches are an example. The extent to which the common law as developed thus far in this country protects other forms of invasion of privacy is not a matter arising in the present case. **It does not arise because, although pleaded more widely,** Miss Campbell's common law claim was throughout presented in court exclusively on the basis of breach of confidence, that is, the wrongful *publication* by the 'Mirror' of private *information.*

16. The European Convention on Human Rights, and the Strasbourg jurisprudence, have undoubtedly had a significant influence in this area of the common law for some years. The provisions of article 8, concerning respect for private and family life, and article 10, concerning freedom of expression, and the interaction of these two articles, have prompted the courts of this country to identify more clearly the different factors involved in cases where one or other of these two interests is present. Where both are present the courts are increasingly explicit in evaluating the competing considerations involved. When identifying and evaluating these factors the courts, including your Lordships' House, have tested the common law against the values encapsulated in these two articles. The development of the common law has been in harmony with these articles of the Convention: see, for instance, *Reynolds v Times Newspapers Ltd* [2001] 2 AC 127, 203-204.

.....

22. Different forms of words, usually to much the same effect, have been suggested from time to time. The second Restatement of Torts in the United States (1977), article 652D, p 394, uses the formulation of disclosure of matter which 'would be highly offensive to a reasonable person'. In *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 185 ALR 1, 13, para 42, Gleeson CJ used words, widely quoted, having a similar meaning. This particular formulation should be used with care, for two reasons. First, the 'highly offensive' phrase is suggestive of a stricter test of private information than a reasonable expectation of privacy. Second, the 'highly offensive' formulation can all too easily bring into account, when deciding whether the disclosed information was private, considerations which go more properly to issues of proportionality; for instance, the degree of intrusion into private life, and the extent to which publication was a matter of proper public concern. This could be a recipe for confusion.

V. Recent trends under American Law

18. The American Constitutional standard of privacy right is wholly inapplicable to the fundamental rights jurisprudence in India. The US Supreme Court has held that people cannot reasonably expect privacy in information they willingly disclose to third parties and, thus, that government intrusions on such information are not Fourth Amendment searches, commonly known as the Third Party Doctrine.[23]

19. In its 1979 decision in **Smith v. Maryland, 442 U.S. 735, 743–44 (1979)**, the Supreme Court ruled in favour of the government, observing that "*this Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.*" The Smith ruling also made reference to another Fourth Amendment case decided three years earlier, **United States v. Miller, 425 U.S. 435 (1976)**, that involved warrantless government access of a suspect's bank records. In Miller supra, the US Supreme Court had also found in favour of the government, holding that:

> *"The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."*

20. The Miller and Smith decisions (supra) manifests what has since become known as the third-party doctrine. Under that doctrine, if you voluntarily provide information to a third party, the Fourth Amendment does not preclude the government from accessing it without a warrant. More

---

[23] Smith v. Maryland, 442 U.S. 735, 743–44 (1979)

succinctly, as the Court held in Smith (supra), you have "no legitimate expectation of privacy" from warrantless government access to that information.

21. In **United States v. Jones, 132 S. Ct. 945, 949 (2012)**, the question involved was GPS tracking performed directly by the government, without a third party intermediary. The government's physical intrusion onto private property, without a valid warrant, to attach a GPS tracker to a suspect's car was in question. The US Supreme Court justices voted unanimously that this was a "search" under the Fourth Amendment, although they were split 5-4 as to the fundamental reasons behind that conclusion. The majority held that by physically installing the GPS device on the defendant's car, the police had committed a trespass against Jones' "personal effects" – this trespass, in an attempt to obtain information, constituted a search per se.

22. As per recent American trends, the American Lower courts have held that historical cell-site location information (CSLI) — a carrier's records of the cell tower used to route a user's calls and messages (typically the tower closest to the user)[24] — is such information willingly disclosed to third parties.[25] Recently, in **United States v. Graham, 824 F.3d 421 (4th Cir. 2016)**, the Fourth Circuit upheld that rule, finding that two defendants could not reasonably expect privacy in CSLI that police used to place them at the crime scene.

23. To further understand the verdict in **United States v. Graham (supra)** it is necessary to understand the factual background that led to the verdict.

---

[24] United States v. Graham, 796 F.3d 332, 343 (4th Cir. 2015).
[25] See, e.g., United States v. Carpenter, 819 F.3d 880, 887–89 (6th Cir. 2016).

a) Aaron Graham and Eric Jordan were prosecuted for six armed robberies in Baltimore that occurred over the course of several weeks in early 2011;

b) The fifth and sixth robberies took place on the same afternoon. Based on eyewitness testimony, the police arrested Graham and Jordan; they then acquired physical evidence connecting the defendants to two of the earlier robberies.

c) While investigating those robberies, an officer seized (under warrant) two phones from Graham's car, linking them to the phone numbers Graham and Jordan gave at arrest.

d) The police sought court orders through the Stored Communications Act (SCA), under which the government may compel disclosure of certain records under a standard lower than probable cause.

e) They demanded that Sprint/Nextel (the defendants' phone carrier) provide the historical CSLI associated with the defendants' phones for a total of 221 days over seven months, collecting over 28,000 CSLI data points for each defendant.

f) Prosecutors used CSLI to place the defendants at most of the crime scenes.

Subsequently, Graham and Jordan brought a motion to suppress the CSLI as the fruit of an unconstitutional search. The district court concluded that the defendants could not legitimately expect privacy in their historical CSLI records as they voluntarily conveyed that information to Sprint/Nextel; the third-party doctrine thus applied. Accordingly, the court rejected the motion, and the defendants were then convicted following a jury trial. They appealed, arguing that the government, by obtaining the CSLI, had violated their Fourth Amendment rights. A panel of the Fourth Circuit agreed.

On appeal, the Fourth Circuit, sitting *en banc* (full bench), reversed the panel's Fourth Amendment holding. Previously in minority, but now in the

majority, Judge Motz first wrote that the third-party doctrine applies even to information conveyed for limited purposes. The Hon'ble court held:

> *"Defendants maintain that cell phone users do not convey CSLI to phone providers, voluntarily or otherwise. We reject that contention. With respect to the nature of CSLI, there can be little question that cell phone users "convey" CSLI to their service providers. After all, if they do not, then who does?*
>
> ....
>
> *... user therefore "conveys" the location of the cell towers his phone connects with to his provider whenever he uses the provider's network.*
>
> ...
>
> *There is similarly little question that cell phone users convey CSLI to their service providers "voluntarily."*
>
> ...
>
> *When an individual purchases a cell phone and chooses a service provider, he expects the provider will, at a minimum, route outgoing and incoming calls and text messages. As most cell phone users know all too well, proximity to a cell tower is necessary to complete these tasks. Anyone who has stepped outside to "get a signal," or has warned a caller of a potential loss of service before entering an elevator, understands, on some level, that location matters.*
>
> ....
>
> *If it were otherwise, courts would frequently need to parse business records for indicia of what an individual knew he conveyed to a third party.* ***For example, when a person hands his credit card to the cashier at a grocery store, he may not pause to consider that he is also "conveying" to his credit card company the date and time of his purchase or the store's street address. But he would hardly be able to use that as an excuse to claim an expectation of privacy if those pieces of information appear in the credit card company's resulting records of the transaction.*** *Cf. United States v. Phibbs, 999 F.2d 1053, 1077-78 (6th Cir. 1993) (Defendant "did not have both an actual and a justifiable privacy interest in . . . his credit card statements.").*
>
> ....
>
> *In their efforts to avoid the third-party doctrine, Defendants attempt to redefine it. They maintain that the third-party doctrine does not apply to historical CSLI because a cell phone user does not "actively choose[] to share" his location information. Defendants' Br. at 30. Such a rule is nowhere to be found in either Miller or Smith. Moreover, this purported requirement cannot be squared with the myriad of federal cases that permit the government to acquire third-*

party records, even when individuals do not "actively choose to share" the information contained in those records.

....

Thus, the redefinition of the third-party doctrine that Defendants advocate not only conflicts with Supreme Court doctrine and all the CSLI cases from our sister circuits, but is also at odds with other established circuit precedent.

C.

In another attempt to avoid the third-party doctrine, Defendants rely on a factual argument long rejected by the Supreme Court and a series of cases involving the content of communications to support their assertion that historical CSLI is protected by the Fourth Amendment.

First, Defendants emphasize that cell phone use is so ubiquitous in our society today that individuals must risk producing CSLI or "opt out of modern society." Defendants' En Banc Br. at 11. Defendants contend that such widespread use shields CSLI from the consequences of the third-party doctrine and renders any conveyance of CSLI "not voluntary," for "[l]iving off the grid . . . is not a prerequisite to enjoying the protection of the Fourth Amendment." Id.

But the dissenting justices in Miller and Smith unsuccessfully advanced nearly identical concerns.

...

The Supreme Court has thus twice rejected Defendants' theory. Until the Court says otherwise, these holdings bind us.

Second, Defendants rely on cases that afford Fourth Amendment protection to the content of communications to suggest that CSLI warrants the same protection.

...

*The Supreme Court has thus forged a clear distinction between the contents of communications and the non-content information that enables communications providers to transmit the content. CSLI, which identifies the equipment used to route calls and texts, undeniably belongs in the non-content category. As the Sixth Circuit recently recognized, CSLI is non-content information because "cell-site data -- like mailing addresses, phone numbers, and IP addresses -- are information that facilitate personal communications, rather than part of the content of those communications themselves." Carpenter, 2016 WL 1445183, at *4.*

...

Outrage at the amount of information the Government obtained, rather than concern for any legal principle, seems to be at the heart of Defendants' arguments.

...

Defendants' answer appears to rest on a misunderstanding of the analysis embraced in the two concurring opinions in Jones. There, the concurring justices recognized a line between "short- term monitoring of a person's movements on public streets," which would not infringe a reasonable expectation of privacy, and "longer term GPS monitoring," which would. Jones, 132 S. Ct. at 964 (Alito, J., concurring in the judgment); see also id. at 955 (Sotomayor, J., concurring). But Jones involved government surveillance of an individual, not an individual's voluntary disclosure of information to a third party. And determining when government surveillance infringes on an individual's reasonable expectation of privacy requires a very different analysis.

In considering the legality of the government surveillance at issue in Jones, Justice Alito looked to what a hypothetical law enforcement officer, engaged in visual surveillance, could reasonably have learned about the defendant. He concluded that four weeks of GPS monitoring by the government constituted a Fourth Amendment "search" because "society's expectation" had always been "that law enforcement agents and others would not -- and indeed, in the main, simply could not -- secretly monitor and catalogue" an individual's movements in public for very long. Id. at 964 (Alito, J., concurring in the judgment) (emphasis added). In other words, direct surveillance by the government using technological means may, at some point, be limited by the government's capacity to accomplish such surveillance by physical means.[26] However, society has no analogous expectations about the capacity of third parties to maintain business records. Indeed, we expect that our banks, doctors, credit card companies, and countless other third parties will record and keep information about our relationships with them, and will do so for the entirety of those relationships -- be it several weeks or many years. Third parties can even retain their records about us after our relationships with them end; it is their prerogative, and many business-related reasons exist for doing so. ***This is true even when, in the aggregate, these records reveal sensitive information similar to what could be revealed by direct surveillance. For this reason, Justice Alito's concern in Jones is simply inapposite to the third-party doctrine and to the instant case. Here, Defendants voluntarily disclosed all the CSLI at issue to Sprint/Nextel.***

....

[26] We note, though, that such a rule would be unprecedented in rendering unconstitutional -- because of some later action -- conduct that was undoubtedly constitutional at the time it was undertaken. See United States v. Sparks, 750 F. Supp. 2d 384, 392 (D. Mass. 2010), aff'd, 711 F.3d 58 (1st Cir. 2013) (recognizing the aggregation theory as "unworkable" because "conduct that is initially constitutionally sound could later be deemed impermissible if it becomes part of the aggregate").

Intrinsic to the doctrine is an assumption that the quantity of information an individual shares with a third party does not affect whether that individual has a reasonable expectation of privacy.

....

Of course, in the face of rapidly advancing technology, courts must "assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." Kyllo, 533 U.S. at 34. The Supreme Court has long concluded that the third-party doctrine does this. Thus the Court has never held that routing information, like CSLI, shared with third parties to allow them to deliver a message or provide a service is protected under the Fourth Amendment. Perhaps this is implicit acknowledgment that the privacy-erosion argument has a flip-side: technological advances also do not give individuals a Fourth Amendment right to conceal information that otherwise would not have been private.[27]

Moreover, application of the third-party doctrine does not render privacy an unavoidable casualty of technological progress -- Congress remains free to require greater privacy protection if it believes that desirable. The legislative branch is far better positioned to respond to changes in technology than are the courts. *See Jones, 132 S. Ct. at 964 (Alito, J., concurring in the judgment) ("**A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.**"); see also In re Application (Fifth. Circuit), 724 F.3d at 615 (explaining that that the proper "recourse" for those seeking increased privacy is often "in the market or the political process").*

The very statute at issue here, the Stored Communications Act (SCA), demonstrates that Congress can -- and does -- make these judgments. The SCA requires the government to meet a higher burden when acquiring "the contents of a wire or electronic communication" from "a provider of electronic communication service" than when obtaining "a record . . . pertaining to a subscriber . . . or customer" from the provider. 18 U.S.C. § 2703(a), (c) (emphasis added). It requires the executive to obtain judicial approval, as the Government did here, before acquiring even non-content information. Id. § 2703(c), (d). And the SCA is part of a broader statute, the Electronic Communications Privacy Act of 1986 (ECPA), which Congress enacted in the wake of Smith. See Pub. L. No. 99-508, 100 Stat. 1848."

---

[27] For example, the Smith Court noted that, because a phone user who "had placed his calls through an operator . . . could claim no legitimate expectation of privacy" in routing information exposed to that operator, "a different constitutional result" did not follow simply "because the telephone company has decided to automate." Smith, 442 U.S. at 744-45. Similarly here, "a different constitutional result" does not follow because the telephone company has decided to make its phones mobile. Cf. United States v. Skinner, 690 F.3d 772, 778 (6th Cir. 2012) ("Law enforcement tactics must be allowed to advance with technological changes, in order to prevent criminals from circumventing the justice system.").

Judge Wilkinson concurred, writing that decisions regarding the Fourth Amendment's privacy protections should be left to Congress. He held and follows:

> *"**Finally, Congress imparts the considerable power of democratic legitimacy to a high stakes and highly controversial area. The emergence of advanced communication technologies has set off a race between criminal enterprises on the one hand and law enforcement efforts on the other.** Modern communication devices -- even as they abet the government's indigenous tendencies to intrude upon our privacy -- also assist criminal syndicates and terrorist cells in inflicting large-scale damage upon civilian populations. Appellants' strict standard of probable cause and a warrant even for non-content information held by third parties thus risks an imbalance of the most dangerous sort, for it allows criminals to utilize the latest in technological development to commit crime and hamstrings the ability of law enforcement to capitalize upon those same developments to prevent crime. The fact that the appellants in this case were convicted of Hobbs Act violations and brandishing offenses cannot obscure the implications of their proposed standards for much more serious threats down the road.*
>
> .....
>
> *It is human nature, I recognize, to want it all. But a world of total privacy and perfect security no longer exists, if indeed it ever did. We face a future of hard tradeoffs and compromises, as life and privacy come simultaneously under siege. How sad, near the very inception of this journey, for appellants to adopt the most stringent of Fourth Amendment standards, to discard the great values of democratic compromise, and to displace altogether the legislative role."*

However Justice Wynn declined to apply the third party doctrine dissenting with the majority view. These cases show the feasibility of a contextual approach to privacy expectations.

VI. Privacy Rights under Singapore Constitution:-

24. Similarly, in a recent decision rendered by the **Apex Court in Singapore** "privacy" has not been elevated to a constitutionally protected fundamental right. This case considered the same issues which were considered by this Hon'ble court in **Naaz foundation case**. The same is clear from the following extract of the Singapore apex court decision rendered in case of **Lim Meng Suang and another v Attorney-General and another appeal and another,** reported in **[2014] SGCA 53**, which reads as under:-

> *43 The arguments raised by Mr Ravi and by Ms Barker on Art 9 in the present appeals are different.* ***Ms Barker argues that the right to life and personal liberty under Art 9(1) should include a limited right to privacy and personal autonomy allowing a person to enjoy and express affection and love towards another human being.*** *Mr Ravi, on the other hand, contends that s 377A is vague, arbitrary and absurd.*
>
> *44* ***In so far as Ms Barker's arguments are concerned, our view is that the right to privacy and personal autonomy which she canvassed should not be read into the phrase "life or personal liberty" in Art 9(1)for three reasons.***
>
> *48 Ina related vein, foreign cases that have conferred an expansive Constitutional right to life and liberty should be approached with circumspection because they were decided in the context of their unique social, political and legal circumstances. For example, the Supreme Court of India has taken an expansive view of the right to life to include an individual's right to health and medical care. This approach must be understood in the context of India's social and economic conditions (see Yong Vui Kong at[83]–[84]). A similarly broad approach has been adopted in the US because of the due process clauses in the Fifth and Fourteenth Amendments to the US Constitution, which are materially different from our Art 9(1).*
>
> *49* ***Indeed, it is significant that Ms Barker herself conceded that the private law relating to privacy was***

a developing one. It is clear that Lim and Chee (and likewise, Tan in CA 125/2013) cannot obtain by the (constitutional) backdoor what they cannot obtain by the (private law) front door. *Indeed, that would be a wholly inappropriate utilisation of the existing body of Constitutional law (which serves a quite different function). More importantly, as we have already noted above (at [30]), Lim and Chee base their Art 9(1) rights on a narrow conception of the right to privacy, viz, that the right to life and personal liberty under Art 9(1) should include a limited right to privacy and personal autonomy allowing a person to enjoy and express affection and love towards another human being.* ***Once again, such a right ought, in our view, to be developed by way of the private law on privacy instead. Indeed, we also observe that the right claimed by Lim and Chee, although of an apparently limited nature, is, in point of fact, not only vague and general, but also contains within itself (contradictorily) the seeds of an unlimited right.*** *Put simply, such a right could be interpreted to encompass as well as legalise all manner of* ***subjective expressions of love and affection****, which could (in turn) embody content that may be wholly unacceptable from the perspective of broader societal policy. At this juncture, we are, of course, back to "square one", so to speak, for this brings us back (in substance at least) to the issue of whether or not s 377Aought to enforce broader societal morality."*

VII Protection of Privacy Laws by the countries joining European Union

25. Apart from above in the following countries which joined European union and have adopted EU Data Protection Directive 95/46/EC, have the following framework of law for granting privacy to its citizen:-

It deserves to be point out that in the context of EU directive for Data protection, the term "Data" is not restricted to electronic / computer data but the said term is used as an over arching term including privacy of an individual in general. The term "personal data" is defined as under:

> ***"personal data"*** *shall mean any information relating to an identified or identifiable natural persons ("data subject") an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity:*

Country	Legal position
GERMANY	The main legal source of data protection in Germany is the **Federal Data Protection Act** (Bundesdatenschutzgesetz in German) (BDSG) which implements the European data protection directive 95/46/EC. Additionally, each German state has a data protection law of its own. In principle, the data protection acts of the individual states intend to protect personal data from processing and use by public authorities of the states whereas the BDSG intends to protect personal data from processing and use by federal public authorities and private bodies. Enforcement is through the data protection authorities of the German states. The competence of the respective state authority depends on the place of business of the data controller.
UNITED KINGDOM	As a member of the European Union, the United Kingdom implemented the EU Data Protection Directive 95/46/EC in March 2000 through **the Data Protection Act 1998** ('Act'). Enforcement is through the Information Commissioner's Office ('ICO'). In common with the rest of the European Union, the

	United Kingdom will adopt the General Data Protection Regulation ("GDPR") from May 2018. When the United Kingdom leaves the European Union it will, in theory, be free to adopt its own data protection laws. Whilst it is widely expected that the United Kingdom will remain close to the standard set by the GDPR, it is currently too early to predict with any degree of certainty the extent to which future UK data protection laws will diverge from those of the European Union.
FRANCE	**Law No. 78 17 of 6 January 1978 on 'Information Technology, Data Files and Civil Liberty' ('Law')** is the principal law regulating data protection in France. The EU Data Protection Directive 95/46/EC was implemented via Law No. 2004-801 of 6 August 2004 which amended the Law. Enforcement of the Law is principally through the 'Commission Nationale de l'Informatique et des Libertés' (CNIL). The CNIL is responsible for ensuring that information technology remains at the service of citizens, and does not jeopardise human identity or breach human rights, privacy or individual or public liberties.
SWITZERLAND	The processing of personal data is mainly regulated by the **Federal Act on Data Protection of 19 June 1992 ('DPA')** and its ordinances, ie the Ordinance to the Federal Act on Data Protection ('DPO') and the Ordinance on Data Protection Certification ('ODPC'). In addition, the processing of personal data is further restricted by provisions in other laws, mainly with regard to the public sector and regulated markets. It should be noted that a substantial revision of the DPA has just been initiated, the implementation of which is however, not to be expected before 2018. The revision of the DPA aims to strengthen data protection in general and to align the Swiss DPA with the requirements of the EU General Data Protection Regulation ("GDPR"), in order to facilitate compliance of Swiss companies with those aspects of the GDPR that are applicable to controllers or processors outside of the EU.
ITALY	The Italian law applicable on privacy issues is the **Legislative Decree no. 196 of 30 June 2003** (Codice in materia di protezionedeidatipersonali, the 'Privacy Code'). The Privacy Code implements Directives 95/46/EC, 2002/58/EC and 2009/12/EC. As a general rule, processing of personal (non sensitive) data by private entities or profit seeking public bodies is only allowed if the data subject gives his/her express

	consent (Section 23 of the Privacy Code).
SPAIN	As a member of the European Union, Spain formally implemented the EU Data Protection Directive 95/46/EC in November 1999 with the **Special Data Protection Act 1999** (the 'Act', also known as the 'LOPD' in Spain). Nevertheless, from 1992, Spain already had a Data Protection Act ('LORTAD') that was fully consistent with most of the contents of the EU Data Protection Directive 95/46/EC. The Act, simply represents an up-to-date version of LORTAD, rather than being a major change in the legal framework. Enforcement is through the Spanish Data Protection Commissioner's Office ('AEPD'). Its last amendment took place in March 2011.
ICELAND	The governing legislation on data protection is Act **No 77/2000 on the Protection and Processing of Personal Data ('Data Protection Act'),** which implemented EU Data Protection Directive 95/46/EC. All electronic processing of personal data, which falls under the Data Protection Act, must be notified to the Icelandic Data Protection Authority, by the controller of the data, unless an exemption applies.
TURKEY	The Turkish Data Protection Law No. 6698 ('DP Law'), which is based on EU Directive 95/46/EC, came into force on 7 April 2016. In the DP Law, personal data was described as "Any information relating to an identified or identifiable natural person". The new DP Law introduces two bodies to watch over and regulate data processing and transfer activities. These are the Data Protection Board and the Data Protection Authority. The Data Protection Board is an independent decision making body.
NETHERLANDS	The Netherlands implemented the EU Data Protection Directive 95/46/EC on 1 September 2001 with the Dutch Personal Data Protection Act (Wbp). Enforcement is through the Dutch Data Protection Authority (AutoriteitPersoonsgegevens). Unless an exemption applies, data controllers who process personal data by automatic means must notify the AutoriteitPersoonsgegevens so that their processing of personal data may be registered and made public. Changes to the processing of personal data will require the notification to be amended.
BULGARIA	Bulgaria implemented the EU Data Protection Directive 95/46/EC with the Personal Data Protection Act (In Bulgarian:), promulgated in the State Gazette No. 1 of 4 January 2002, as amended periodically (Act). The Act

	came into force on1 January 2002. The Act was last amended by the State Gazette, Issue No. 15 of 15 February 2013. Currently, a new Bulgarian data protection law is in process of discussion and is being prepared by a group of experts, including experts from the the Bulgarian Data Protection Authority. The new law is expected to be adopted by May 2018 and to create a new framework in connection to Regulation (EU) 2016/679. The Bulgarian data protection authority (DPA) is the Personal Data Protection Commission. Unless an exemption applies, prior to initiating any personal data processing data controllers must apply for registration with the DPA. The registration covers the data controller and the personal data registers controlled by it.
FINLAND	Finland is a member of the European Union and has implemented the EU Data Protection Directive 95/46/EC with the Personal Data Act 523/1999 ('Act') (Henkilötietolaki) in June 1999. Other important Finnish laws concerning data privacy and protection are the Code for Information Society and Communications Services 917/2014 ('Information Society Code') (Tietoyhteiskuntakaari) of 1 January 2015, which aims to inter alia ensure the confidentiality of electronic communication and the protection of privacy, and the Act on the Protection of Privacy in Working Life 759/2004 ('Working Life Act') (Lakiyksityisyydensuojastatyöelämässä), which aims to promote the protection of privacy and other rights safeguarding the privacy in working life. Information Society Code is an ambitious effort to collect the relevant laws relating to information society under a single statute. The Information Society Code contains mostly the same provisions as the preceding laws, but it combines a large quantity of different provisions under a single law and covers a large area of legislation. The Working Life Act includes some specific provisions on privacy issues relating to employment and work environments such as right to monitor employees' email communication.
IRELAND	The core Irish data protection law is comprised in the Data Protection Act 1988 ('1988 Act') as amended by the Data Protection (Amendment) Act 2003 ('2003 Act') (together the Data Protection Acts ("DPA")). The 2003 Act implemented the EU Data Protection Directive (95/46/EC) ("Data Protection Directive"). In addition to the DPA, the European Communities (Electronic

	Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 ('ePrivacy Regulations') set out data protection rules in relation to direct marketing and electronic networks and services, including location data and cookies.

VIII Analysis of laws pertaining to privacy in countries where right to privacy has been established under their respective Constitution:-

Country	Legal position
RUSSIA	Fundamental provisions of data protection law in Russia can be found in the Russian Constitution, international treaties and specific laws. Russia is a member of the Strasbourg Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention) (ratified by Russia in 2006) and the Russian Constitution establishes the right to privacy of each individual (articles. 23 and 24). Most rules are found in specific legislation, particularly the Data Protection Act No. 152 FZ dated 27 July 2006 (DPA) and various regulatory acts adopted to implement the DPA as well as other laws, including the Information, Information Technologies and Information Protection Act No. 149 FZ dated 27 July 2006 establishing basic rules as to the information in general and its protection. In addition, the Russian Labour Code contains provisions on the protection of employees' personal data (Part XIV). Other laws may also contain data protection provisions which implement the provisions of DPA in relation to specific areas of state services or industries. On 22 July 2014 notable amendments to the DPA were adopted and came into force on 1 September 2015. The amendments require all personal data operators to store and process any personal data of Russian individuals within databases located in Russia (subject to few exceptions). The penalty for violation of this requirement is ultimately the blocking of websites involving unlawful handling of Russian personal data. A Register of Infringers of Rights of Personal Data Subjects shall be established by the Roscomnadzor and from there and the Roscomnadzor may move to block websites.
CHILE	Personal Data Protection is addressed in several specific laws, as well as scattered provisions in related or complementary laws and other legal authority: ➢ Constitution of the Republic of Chile, Art. 19 N° 4: establishes the 'respect and protection of the public and private life, and the honour of the person and its family'. Any person who by arbitrary or illegal Act or omission suffers a deprivation, perturbation or threat to this right

	may file a Constitutional Protection Action. ➢ Law 19,628 'On the protection of private life', commonly referred as 'Personal Data Protection Law' (PDPL): mainly defines and refers to the treatment of personal information in public and private databases. Last modified: Feb. 17, 2012. ➢ Law 20,285, 'On the Access to Public Information': sets forth the Public Function Transparency Principle, the individual right to access the information of Public Administration bodies, and the procedures and exceptions thereof. ➢ Law 20,575: 'Establishes the Destination Principle on the Treatment of personal data': incorporates additional rules when treating economic and debt-related personal data. ➢ General Law on Banks, article 154, establishes the Banking Secrecy: holds that, subject to certain specific exemptions, all deposits are secret, and related information can be given only to the account's owner or designated representative. ➢ Law 19,223, 'Criminal Conducts related to Informatics': establishes sanctions for those who breach and unlawfully access and/or use the information available in electronic databases.
ARGENTINA	Section 43 of the Federal Constitution grants citizens expeditious judicial action to gain access to information about them contained in public and private databases and to demand its amendment, updating, confidentiality, or suppression if it is incorrect. Personal Data Protection Law Number 25,326 (the 'PDPL'), enacted in October 2000, provides much broader protection of personal data closely following Spain's data protection law. On 30 June 2003, the European Commission recognised that Argentina provides an 'adequate' level of protection of personal data, in line with the Data Protection Directive (95/46/EC).
THAILAND	At present, Thailand does not have any general statutory law governing data protection or privacy. However, the Constitution of the Kingdom of Thailand does recognize the protection of privacy rights. In addition, statutory laws in some specific areas (such as telecommunications, banking and financial businesses (Specific Businesses) as well as other non-business related laws, such as certain provisions under Thai

	Penal Code and the Child Protection Act B.E. 2543 (2003), do provide a certain level of protection against any unauthorised collection, processing, disclosure and transfer of personal data. Recently, the draft Personal Information Protection Act ('Draft'), which has been reviewed by the Council of State, was given to the Committee for House of Representative Coordination to review and analyse if there are any practical issues on applying the law and how the Data Protection Committee should be formed. The Draft is being reviewed by the Office of the Public Sector Development Commission and will be submitted to the Cabinet for approval later. The current Draft provides protection of personal data by restricting the gathering, using, disclosing and altering of any personal data without the consent of the data owner. The Draft also imposes both criminal penalties and civil liability for any violation of the Draft and calls for the establishment of a Protection of Personal Data Commission to regulate compliance with the Draft.
COLOMBIA	Article 15 of the Colombian Constitution sets forth fundamental rights to intimacy, good name or reputation and data protection. Law 1266/08 ('Law 1266'), reviewed by the Colombian Constitutional Court in Decision C 1011/08, regulates the collection, use and transfer of personal information regarding monetary obligations related to credit, financial and banking services. Law 1581 of 2012 ('Law 1581'), reviewed by the Colombian Constitutional Court in Decision C-748/11, contains comprehensive personal data protection regulations. This law is intended to implement the Constitutional right to know, update and rectify information gathered about them in databases or files, enshrined in Article 20 of the Constitution, as well as other rights, liberties and Constitutional guarantees referred to in Article 15 of the Constitution.

IX. Vague concept cannot be elevated to a fundamental right status

26. It is submitted that before elevation of any concept/statutory right to the status of a "protected and enforceable Constitutional fundamental right", it is essential to lay down its contours, so as to enable the state, as well as individuals, to precisely measure as to what aspect/action the said fundamental right seeks to protect. If the said right would not be able to clearly spell out as to what action/aspect it seeks to protect, protection of the same by the state would become impossible and importantly there would be no "judicially discernible and manageable standard" to protect and enforce the said right.

27. If right to privacy [statutorily protected under various statutes with specificities] is conferred a status of constitutionally enforceable and protected and undefined fundamental right, then it would have both *private law* as well as *public law* implications. In such a scenario the State will have to protect such undefined and subjective individual specific right of each individual from other private individuals also. The authorities which are "state" within the meaning of Article 12 including private entities discharging "public functions" will be amenable to and answerable for an alleged violation of a right which an individual - in his own subjective manner – treats to be his right of "Privacy".

Protection of the said right of an individual from another individual will become impossible, as, such another individual will not be able to know with reasonable certainty as to what, in this regard, are the limits of his lawful conduct which he must not transgress. Similar would be the position of state inasmuch as in such a situation, state would also not know to as what aspect of human conduct would be constitutionally protected and what aspect can be legitimately regulated by the state. In such an ambiguous state possibility

of the State inadvertently violating either privacy of such other individual or perceived subjective privacy of such individuals cannot be ruled out.

28. If this ambiguous, vague and uncertain subjective concept of "privacy" is conferred Constitutional status of protected fundamental right then the state will be mandated to enforce it. It is most important to note that if the said right is declared to be a Fundamental Right, the State may have to provide for penal consequences for breach thereof. Also for breach thereof, the state will have to provide for penal provision.

In this context, it has been well settled by a series of judicial decision rendered by this Hon'ble court that a vague and uncertain law cannot remain in the statute book. Reliance in this regard is placed on the judgment of this Hon'ble court rendered in ***A.K. Roy v. Union of India,*** reported in **(1982) 1 SCC 271** wherein this Hon'ble court held as under:-

> ***61.*** *In making these submissions counsel seem to us to have overstated their case by adopting an unrealistic attitude. It is true that the vagueness and the consequent uncertainty of a law of preventive detention bears upon the unreasonableness of that law as much as the uncertainty of a punitive law like the Penal Code does.* ***A person cannot be deprived of his liberty by a law which is nebulous and uncertain in its definition and application.*** *But in considering the question whether the expressions aforesaid which are used in Section 3 of the Act are of that character, we must have regard to the consideration whether the concepts embodied in those expressions are at all capable of a precise definition. The fact that some definition or the other can be formulated of an expression does not mean that the definition can necessarily give certainty to that expression. The British Parliament has defined the term 'terrorism' in Section 28 of the Act of 1973 to mean "the use of violence for political ends", which, by definition, includes "any use of violence for the purpose of putting the public or any section of the public in fear". The phrase 'political ends' is itself of an uncertain character and comprehends within its scope a variety of nebulous situations. Similarly, the definitions contained in Section 8(3) of the Jammu & Kashmir Act of 1978 themselves depend upon the meaning of concepts like "overawe the government".* ***The formulation of definitions cannot be a panacea to the evil of vagueness and uncertainty.*** *We do not, of course, suggest that the legislature should not attempt to define*

or at least to indicate the contours of expressions, by the use of which people are sought to be deprived of their liberty. The impossibility of framing a definition with mathematical precision cannot either justify the use of vague expressions or the total failure to frame any definition at all which can furnish, by its inclusiveness at least, a safe guideline for understanding the meaning of the expressions used by the legislature. ***But the point to note is that there are expressions which inherently comprehend such an infinite variety of situations that definitions, instead of lending to them a definite meaning, can only succeed either in robbing them of their intended amplitude or in making it necessary to frame further definitions of the terms defined.*** *Acts prejudicial to the 'defence of India', 'security of India', 'security of the State', and 'relations of India with foreign powers' are concepts of that nature which are difficult to encase within the strait-jacket of a definition. If it is permissible to the legislature to enact laws of preventive detention, a certain amount of minimal latitude has to be conceded to it in order to make those laws effective. That we consider to be a realistic approach to the situation. An administrator acting bona fide, or a court faced with the question as to whether certain acts fall within the mischief of the aforesaid expressions used in Section 3, will be able to find an acceptable answer either way. In other words, though an expression may appear in cold print to be vague and uncertain, it may not be difficult to apply it to life's practical realities. This process undoubtedly involves the possibility of error but then, there is hardly any area of adjudicative process which does not involve that possibility.*

62. *The requirement that crimes must be defined with appropriate definiteness is regarded as a fundamental concept in criminal law and must now be regarded as a pervading theme of our Constitution since the decision in Maneka Gandhi[Maneka Gandhi v. Union of India, (1978) 2 SCR 621 : (1978) 1 SCC 248 : AIR 1978 SC 597] .* ***The underlying principle is that every person is entitled to be informed as to what the State commands or forbids and that the life and liberty of a person cannot be put in peril on an ambiguity.*** *However, even in the domain of criminal law, the processes of which can result in the taking away of life itself, no more than a reasonable degree of certainty has to be accepted as a fact.* ***Neither the criminal law nor the Constitution requires the application of impossible standards and therefore, what is expected is that the language of the law must contain an adequate warning of the conduct which may fall within the proscribed area, when measured by common understanding.*** *In criminal law, the legislature frequently uses vague expressions like 'bring into hatred or contempt', or 'maintenance of harmony between different religious groups', or 'likely to cause disharmony or ... hatred or ill will', or 'annoyance to the public' [see Sections 124-A, 153-A(1)(b), 153-B(1)(c), and 268 of the Penal Code]. These expressions, though they are difficult to define, do not elude a just application to practical situations. The use of language carries with it the inconvenience of the imperfections of language.*

29. Similarly this Hon'ble court in the case of ***Shreya Singhal v. Union of India,*** reported in **(20015) 5 SCC 1** held as under:-

> *"55.* ***The US Supreme Court has repeatedly held in a series of judgments that where no reasonable standards are laid down to define guilt in a section which creates an offence, and where no clear guidance is given to either law abiding citizens or to authorities and courts, a section which creates an offence and which is vague must be struck down as being arbitrary and unreasonable.*** *Thus, in Musser v. Utah [92 L Ed 562 : 68 S Ct 397 : 333 US 95 (1948)] , a Utah statute which outlawed conspiracy to commit acts injurious to public morals was struck down.*
>
> *85.* ***These two cases illustrate how judicially trained minds would find a person guilty or not guilty depending upon the Judge's notion of what is "grossly offensive" or "menacing".*** *In Collins case, both the Leicestershire Justices and two Judges of the Queen's Bench would have acquitted Collins whereas the House of Lords convicted him. Similarly, in the Chambers case, the Crown Court would have convicted Chambers whereas the Queen's Bench acquitted him.* ***If judicially trained minds can come to diametrically opposite conclusions on the same set of facts it is obvious that expressions such as "grossly offensive" or "menacing" are so vague that there is no manageable standard by which a person can be said to have committed an offence or not to have committed an offence.*** *Quite obviously, a prospective offender of Section 66-A and the authorities who are to enforce Section 66-A have absolutely no manageable standard by which to book a person for an offence under Section 66-A. This being the case, having regard also to the two English precedents cited by the learned Additional Solicitor General, it is clear that Section 66-A is unconstitutionally vague.*

30. The concept of privacy is so inherently vague, uncertain, elastic and subjective that in no circumstance it can convey an adequate warning of the conduct which may fall within the proscribed area, when measured by common understanding. Furthermore, it is also clear that even judicially trained minds have also come to diametrically opposite conclusions on the same set of facts, while dealing with the cases of personal privacy that it makes it obvious that expressions *"privacy is so vague that there is no manageable standard by which a person can be said to have committed an breach or not to have committed a breach of the said concept.*

X. Privacy is not a fundamental right but only a legitimate claim/interest covered by the Constitutional ethos having sanction of Common Law - Every such claim or interest of the society/individual cannot be elevated to the status of fundamental right

31. Conceptually, every human desire, if interpreted liberally can be traced to the language used in Article 21 of Indian Constitution. However, not every human desire can be guaranteed and or protected under the said Article. The concept of privacy, both in private law field as well in public law field is at the best a legitimate "claim" or an "interest" having sanction of Common Law. It is respectfully submitted that any such "claim" or "interest" which have sanction of common law and are relatable to any of the guaranteed fundamental rights under our constitution cannot, by way of judicial interpretation, be elevated to the status of an independent fundamental right enforceable directly by the Constitutional Courts including this Hon'ble Court under Article 32 of the Constitution.

32. That is so, because these common law "interest" or "claims" have both positive, as well as, negative obligation and implication in private as well as public law spheres. That is to say that these common law "interest" or "claims", on occasion can have positive impact on state and society which promotes constructive/positive development of state laws, individuals and society. Whereas, at the same time it can have negative impact/implication on state and society, which thus impairs constructive and positive development of state laws, individuals and society.

33. It is respectfully submitted that wherever and whenever such "claim" or "interests" have a negative obligation/implication on constructive development of society/individual, it cannot be conferred with the status of protected fundamental right, as it is deemed that guaranteed fundamental

rights only have positive obligations qua individuals and State and have no negative impact/implication on constructive development of society/individual.

34. In such circumstances, it becomes a policy decision to ascertain as to which part of the activity has a positive obligation towards state and fellow individuals and thus requires protection and which part of the activity has a negative implication on betterment and constructive development of the state and its citizens and thus requires to be declared as outlawed.

35. Thus ascertainment and delineation of this positive obligation viz negative implication on state and its citizens, being essentially a policy decision, should be best left to legislature to be protected and or regulated through statutory framework. It is submitted that if such common law claims and interests are conferred the status of an overarching protected fundamental right, by way of judicial interpretation then it would amount to this Hon'ble court venturing into a policy making decision, which is impermissible in law. It is submitted that by application of "doctrine of Constitutional implication/limitation" this Hon'ble court has in past also refrained from declaring any new specie of fundamental right which though was directly relatable to the existing fundamental rights guaranteed under Part III of Indian Constitution. Illustratively the said examples are as under:-

a) Article 21 expressly provides for positive obligation of 'right to life' but the said the guaranteed "right to life" does not include within its gamut "right to die" as it had a negative implication/impact on society and state. It is stated that though this claim of "right to die" can be easily read into or can be said to be inextricably relatable to right to life protected under Article 21, since this "right to die" was considered to be

having a negative impact/implication on the society, this Hon'ble Court (though the Constitution bench of this Hon'ble court is seized of the said matter) has left it to the competent Legislature to come up with the suitable legislation either expressly accepting such claim and protecting the same through statutory provisions or rejecting the said claim.

b) Similarly, the claim of "right to know" has been traced to Article 19 (1) (a) of the Constitution, however, since this claim of "right to know" also had a negative application/implication of not to know about the personal information of fellow citizens, therefore, it was left by this Hon'ble court for competent legislature come up with a statutory framework to statutorily regulate the said right to know. The said "right to know" which can be traced to Article 19 (1) (a) of the Constitution is therefore now regulated through provisions of Right to Information Act.

c) Likewise, right to education was read by this Hon'ble Court as a fundamental right guaranteed under Article 21 of the Constitution in the case of *Unni Krishnan vs State of A.P.* reported in *(1993) 1 SCC 645.* However, in the year 2002 when legislature deemed it fit and proper, it was specifically declared by the legislature as guaranteed fundamental right by way of a Constitutional amendment. Furthermore, the said right was conferred subject of condition that the right to free and compulsory education would be extended not to every individual but only to children of age between 6 years to 14 years in such manner as determined by the state through appropriate law.

XI Dangers of expanding the meaning of rights conferred under Part III of our Constitution

36. It is submitted that there are inherent dangers in conferring an expansive meaning to rights guaranteed under Part III of the Constitution which can be illustratively brought out through following examples:

37. It is submitted that right to life guaranteed under article 21 also includes "right to defend" once on body. "Right to Defend one's own body" is also a very valuable and natural right. Further, this right has been and established common law right. Thus in this context juxtaposed with the scheme of our Indian constitution, can somebody be permitted to argue that "right to defend" is an inextricably linked facet to right to life guaranteed under Article 21 of the Indian Constitution and to secure his life he has a "right to keep a firearm and/or maintain a militia" on the pretext that the same is a natural right and also a common law right. Thus on this pretext can any person seek creation of a new fundamental right to keep arms and ammunition through judicial interpretation by arguing that the same is a facet of right to life guaranteed under Article 21 and this right is already a recognised common law right and has been specifically guaranteed under other jurisdiction of the worlds eg. US Constitution by way of Second amendment.

38. Similarly, forensic analysis of genetic material is an accepted mode of criminal investigation. For example Fingerprints analysis of a suspect, semen analysis to identify rape accused are effective procedures which are employed by investigating agencies to bring a criminal to book. It is submitted that giving expansive meaning to the rights conferred under Part III, it is possible for a criminal to argue that their biometric and genetic material is private to them and using the same in criminal investigation against them would amount to violation of right against self-incrimination.

39. Thus it is respectfully submitted that any "claim" or "interest" which has a negative implication on the society and which though may appear to be necessary concomitant for exercise of already declared fundamental rights under part III of our constitution or are concepts which appears to be relatable to fundamental rights already guaranteed under part III of our constitution, cannot be conferred with the status of an independent fundamental right enforceable through article 32 of the Constitution of India.

It is submitted that in such scenario it should be best left with the competent legislature to come up with suitable regulatory mechanism for first delineating such legitimate claims or interest which are necessary for constructive development of our Constitutional ethos.

It is submitted that in this context the doctrine of Constitutional implication would squarely apply. Reliance in this regard is placed on judgment of this Hon'ble court rendered in ***Manoj Narula v. Union of India,*** reported in **(2014) 9 SCC 1** wherein this Hon'ble court held as under:-

> ***Doctrine of Constitutional implications***
>
> ***71.*** *Dixon, J., in Australian National Airways Pty. Ltd. (No. 1) v. Commonwealth [(1945) 71 CLR 29 at p. 85 (Aust)] , said: "I do not see why we should be fearful about making implications". The said principle has been approved in Lamshed v. Lake [(1958) 99 CLR 132 at pp. 144-5 (Aust)] , and thereafter, in Payroll Tax case [Victoria v. Commonwealth, (1971) 122 CLR 353 at p. 401 (Aust)] . Thus, the said principle can be taken aid of for the purpose of interpreting Constitutional provision in an expansive manner. But, it has its own limitations. The interpretation has to have a base in the Constitution. The Court cannot rewrite a Constitutional provision. In this context, we may fruitfully refer to Kuldip Nayar case [Kuldip Nayar v. Union of India, (2006) 7 SCC 1] wherein the Court repelled the contention that a right to vote invariably carries an implied term i.e. the right to vote in secrecy. The Court observed that where the Constitution thought it fit to do so, it has itself provided for elections by secret ballot e.g. in the case of election of the President of India and the Vice-President of India. Thereafter, the Court referred to Articles 55(3) and 66(1) of the Constitution which provide for elections*

of the President and the Vice-President respectively, referring to voting by electoral colleges, consisting of elected Members of Parliament and Legislative Assembly of each State for the purposes of the former office and Members of both Houses of Parliament for the latter office and in both cases, it was felt necessary by the Framers of the Constitution to provide that the voting at such elections shall be by secret ballot through inclusion of the words "and the voting at such election shall be by secret ballot". If the right to vote by itself implies or postulates voting in secrecy, then Articles 55(3) and 66(1) would not have required the inclusion of such words. The necessity for including the said condition in the said Articles shows that "secret ballot" is not always implied. It is not incorporated in the concept of voting by necessary implication. Thereafter, the Court opined: (Kuldip Nayar case[Kuldip Nayar v. Union of India, (2006) 7 SCC 1] , SCC p. 139, para 424)

> *"424. It follows that for 'secret ballot' to be the norm, it must be expressly so provided. To read into Article 80(4) the requirement of a secret ballot would be to read the words 'and the voting at such election shall be by secret ballot' into the provision. To do so would be against every principle of Constitutional and statutory construction."*

75. *The principle of Constitutional morality basically means to bow down to the norms of the Constitution and not to act in a manner which would become violative of the rule of law or reflectible of action in an arbitrary manner. It actually works at the fulcrum and guides as a laser beam in institution building. The traditions and conventions have to grow to sustain the value of such a morality. The democratic values survive and become successful where the people at large and the persons in charge of the institution are strictly guided by the Constitutional parameters without paving the path of deviancy and reflecting in action the primary concern to maintain institutional integrity and the requisite Constitutional restraints. Commitment to the Constitution is a facet of Constitutional morality. In this context, the following passage would be apt to be reproduced:*

> *"If men were angels, no Government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place oblige it to control itself. A dependence on the people is, no doubt, the primary control on the government; but experience has taught mankind the necessity of auxiliary precautions. [James Madison as Publius, Federalist 51] "*

XII. <u>The technological advancement should be used for "good governance" and the privacy issues need to be taken care of by Statutes</u>

40. The rapidly increasing technological advancement globally and more particularly in electronic and communications field has opened several new vistas. At the hands of handful of individuals, no attempt be permitted which defeats positive and constructive efforts for "good governance" in a developing country like India on an ostensible ground of "privacy" which can be adequately taken care of by statutory provisions.

41. India is a country where substantial number of population either lives below the poverty line or just above the poverty line. Even basic necessities like food, drinking water, seeds, fertilizers, agricultural equipments and banking has not reached them

42. Though, this Hon'ble Court is not examining validity of Aadhar, the following facts need to be examined to satisfy the judicial conscience of this Hon'ble Court that if privacy is declared to be a Fundamental Right [which can always be secured by statutory provisions] all out attempts will be made to stop 'good governance' and majority of the deprived population of the country would suffer.

43. Aadhar card / number is the most widely held form of identity document with the widest coverage amongst the residents / citizens of India. This is evident from the following chart:

Identity Document	Coverage
Passport	6.9 Cr.
Pan Card	29 Crore [Approx.]
EPIC Card	60 Crores [Approx.]

Ration Card	15.17 Crore [Approx.]
Driving License	17.37 Crore [Approx.]
Aadhar	**115.15 Crore**

44. The use of Aadhar is one of the classic case of good governance which can be demonstrated by one illustration. By using Aadhar Card, the total recorded savings of the Government of India from just one scheme viz. the Direct Benefit Transfer Scheme [based upon Aadhar] has been **Rs.49,560 crores** in just two years i.e. 2014-15 and 2015-16.

45. This not only serves public interest but the intended benefits, subsidies and services offered by the Government as a welfare State [which is its Constitutional duty] reaches to correct beneficiaries weeding out fake and duplicate beneficiaries saving thousand and crores of rupees.

46. This Honbel Court in the case of *PUCL vs Union of India (2011) 14 SCC 331* has approved the recommendations of the High Powered Committee headed by Justice D.P. Wadhwa, which recommended linking of Aadhar with PDS and has encouraged State Governments to adopt the same.

47. This Hon'ble Court in State *of Kerala & ors. Vs President Parents Teachers Association, SNVUP and Ors. (2013) 2 SCC 705* has directed use of Aadhar for checking bogus admissions in schools with the following observations:

> *"18. We are, however, inclined to give a direction to the Education Department, State of Kerala to forth with give effect to a circular dated 12.10.2011 to issue UID Card to all the school children and follow the guidelines and directions contained in their circular. Needless to say, the Government can always adopt, in future, better scientific methods to curb such types of bogus admissions in various aided schools."*

48. This Hon'ble Court, while monitoring the PILs relating to night shelters for the homeless and right to food through the public distribution system, has lauded and complimented the effort of State Governments for, inter alia, carrying out biometric identification of the head of family of each household to eliminate fictitious, bogus and ineligible BPL / AAY household cards. This is evident from the following extracts in PUCL vs Union of India (2010) 13 SCC 45

> *48. In the affidavit, it is mentioned that NGO, Samya had conducted survey and identified 15,000 homeless beneficiaries of which 14,850 which have been approved for giving "homeless cards". These cards are being prepared zonewise and the list is displayed at the office of the Assistant Commissioners/Circle Office for distribution of the special homeless cards to the beneficiaries after obtaining their biometric impressions. The NGO, Samya has also been informed to facilitate delivery of these cards to the beneficiaries and enable them to lift the specified food articles and kerosene oil allocated from the linked fair price shop/kerosene oil depot. The details have been mentioned in the AAY programme.*
>
> *49. It is mentioned in the affidavit that under the Central Scheme of Food and Supplies Department, Government of NCT of Delhi is carrying out review of BPL/AAY household cards which were issued before 15-1-2009. It is simultaneously carrying out biometric identification of head of family of each household to eliminate fictitious, bogus and ineligible cards and those who have left Delhi.*
>
> *53. The Delhi Government has very minutely and carefully analysed the problems of homeless people living in these shelters and is trying to provide a comprehensive programme for the homeless. We must compliment the Government of NCT of Delhi for this effort. We would like the Government of NCT of Delhi to file a further affidavit indicating what progress has been made on different fronts.*

49. Similarly, this Hon'ble Court in PUCL [PDS matters] vs Union of India & ors. (2013) 14 SCC 368 had held <u>that computerisation is going to help the public distribution system in the country in a big way and encouraged and endorsed the digitization of database including biometric identification of the beneficiaries</u>. In fact this Hon'ble Court had requested Mr. Nandan Nilekani, the then Chairman, UIDAI to suggest ways in which the computerisation

process of PDS can be expedited. The following extracts from the abovementioned order is relied upon :

> *2. There seems to be a general consensus that computerisation is going to help the public distribution system in the country in a big way. In the affidavit it is stated that the Department of Food and Public Distribution has been pursuing the States to undertake special drive to eliminate bogus/duplicate ration cards and as a result, 209.55 lakh ration cards have been eliminated since 2006 and the annual saving of foodgrain subsidy has worked out to about Rs 8200 crores per annum. It is further mentioned in the affidavit that end-to-end computerisation of public distribution system comprises creation and management of digitised beneficiary database including biometric identification of the beneficiaries, supply chain management of TPDS commodities till fair price shops.*
>
> *3.It is further stated in the affidavit that in the State of Gujarat, the process of computerisation is at an advanced stage where issue of bar coded ration cards has led to a reduction of 16 lakh ration cards. It is expected that once the biometric details are collected, this number would increase further. For the present, a reduction of 16 lakh ration cards would translate into an annual saving of over Rs 600 crores. This is just to illustrate that computerisation would go in a big way to help the targeted population of the public distribution system in the country.*
> *4. In the affidavit it is further mentioned that the Government of India has set up a task force under the Chairmanship of Mr Nandan Nilekani, Chairman, UIDAI, to recommend, amongst others, an IT strategy for the public distribution system. We request Mr Nandan Nilekani to suggest us ways and means by which computerisation process of the public distribution system can be expedited. Let a brief report/affidavit be filed by Mr Nandan Nilekani within four weeks from today.*

50. This Hon'ble Court in PUCL vs Union of India (2010) 5 SCC 318 has also endorsed biometric identification of homeless persons so that the benefits like supply of food and kerosene oil available to persons who are below poverty line can be extended to the correct beneficiaries.

51. Recently, this Hon'ble Court in the case of Lokniti Foundation vs Union of India vide order dated 6.2.2017 passed in Writ Petition No.607 of 2016 has approved Aadhar based verification of existing and new mobile phone number subscribers. This is a great leap towards anonymous pre-paid sim cards which are being used either for terrorist activities or for such other similar illegal activities.

52. The fact that food security is one of the most prime concern of the Central Government which is under a mandate of National Food Security Act, 2013 also **statutorily incorporates Aadhar**, would show that not only public interest is involved [as against a perceived and subjective privacy interest of few individuals] but declaration of privacy as Fundamental Right would open several other statutes to the vulnerability of challenge. **Section 12 of the National Food Security Act, 2013** reads as under

> ***"REFORMS IN TARGETED PUBLIC DISTRIBUTION SYSTEM***
>
> *12. (1) The Central and State Governments shall endeavour to progressively undertake necessary reforms in the Targeted Public Distribution System in consonance with the role envisaged for them in this Act.*
>
> *(2) The reforms shall, inter alia, include—*
>
> *(a) doorstep delivery of foodgrains to the Targeted Public Distribution System outlets;*
> *(b) application of information and communication technology tools including end-to-end computerisation in order to ensure transparent recording of transactions at all levels, and to prevent diversion;*
> *(c) leveraging "aadhaar" for unique identification, with biometric information of entitled beneficiaries for proper targeting of benefits under this Act; "*

53. Therefore, it is humbly submitted that when Aadhaar has been adopted by several statutes and authorities across the country both pursuant to directions by this Hon'ble Court as well as legislative amendments passed by the Parliament of India, this Hon'ble Court may not elevate a statutory right to the level of fundamental right which will open doors for challenge to various public interest enactments.

54. The amended Section 139AA of the Income Tax Act which intends to expose all shell companies and curb the menace of black money, money laundering and tax evasion is already held to be Constitutional by this Hon'ble Court on the challenge of Article 14 and 19 of the Constitution in *Binoy Viswam v. Union of India & Ors.*, W.P. (C) 247 of 2017 dated 09.06.2017.

55. The object and purpose of the said amendment is also approved by this Hon'ble Court in the aforesaid judgment. Such a salutary provisions eradicating shell companies, black money and money laundering would also come under the vulnerability of being declared ultra vires. Right to Privacy is declared to be a Fundamental Right.

This is more particularly so when otherwise the Income Tax Act provides for sufficient statutory safeguards for protection of privacy.

56. When the technological advancement are taking place globally and virtually on daily basis, the Government/(s) as welfare State functioning under the constitution may come up with several regulations / programmes / schemes in the direction of good governance. Just to give an illustration, it may be pointed out that in large number of rural schools, it is found that qualified teachers appointed never come for teaching. Their fake presence is marked and a local unqualified person staying in the village teaches the students. If, in future, the presence of the qualified teachers is linked with either Aadhar or such similar identification, it would be a great leap in the direction of imparting education in rural areas.

57. There can be several such areas where the technology can be used for larger public good and in furtherance of "good governance" while protecting the individual privacy based upon each subject being dealt with by way of a Statute.

XIII Reliance placed by the petitioners on the case law existing in other jurisdictions to interpret the Indian Constitution merits rejection

58. It is further submitted that reliance placed by the petitioners on the case law existing in other jurisdictions to interpret the Indian Constitution is liable to be rejected. It is respectfully submitted that in view of the prevailing situation, it will not be in the interest of social fabric of the country and also in the interest of justice that Indian Constitution is interpreted in light of Constitutional law prevailing in USA or any other foreign country, which has expressly provided in its Constitution a right of privacy.

59. It is submitted that in absence of the parliament in its wisdom, creating fundamental right of privacy the said right cannot be read into the Constitution even by application of doctrine of "sub-silentio" or "Constitutional silence". A fortiori creating a right of privacy by interpreting the Indian Constitution in the light of the case law existing in American or any other foreign jurisdiction, will amount to doing violence with the conscious language of the Constitution.

It is submitted that that the thought process of Indian citizens, their societal behaviour, their socio-economic problems etc. are different from the problems of citizens living in western countries. Their concept of privacy is strikingly different from the privacy standards prevailing in western countries. As such the standards of privacy existing in western countries ought not be embodied in Indian Constitution as the Indian Constitution shall have to be interpreted strictly in Indian context and keeping the citizens of India in mind.

60. The aforesaid principle has been duly recognised in catena of judgements rendered by this Hon'ble court, relevant portions of which reads as under:-

i) In the case of ***Joseph Kuruvilla Vellukunnel v. Reserve Bank of India,*** reported in **1962 Supp (3) SCR 632 : AIR 1962 SC 1371,** this Hon'ble court held as under:-

> ***50.*** *Mr Nambiar, however, joined issue on the use of the American precedents on the ground that banking in America is by grace of legislature, and is either a franchise or a privilege, which has no place in our Constitution. He added that the carrying on of business is not one of the provisions of the American Bill of Rights, nor a fundamental right, as we understand it, though by judicial construction the individual right has been brought within the Fourteenth Amendment. He, therefore, contended that American cases and American laws should not be used. In our opinion, no useful purpose will be served by trying to establish the similarities or discrepancies between the American Constitution and banking laws, on the one hand, and our Constitution and our banking laws, on the other, and we do not wish to rest our decision on the American and Japanese analogies.*
>
> ***75.*** *The aid of American concepts, laws and precedents in the interpretation of our laws is not always without its dangers and they have therefore to be relied upon with some caution if not with hesitation because of the difference in the nature of those laws and of the institutions to which they apply. Mr Nambiyar relied upon these different concepts and submitted that in U.S.A. the right to carry on business is not a fundamental right but is a "franchise", though, it has by legal interpretation, been brought within the fourteenth amendment and the doctrine of "franchise" has no place in the Indian Constitution: C.S.S. Motor Service v. State of Madras [ILR (1953) Mad. 304] approved in Saghir Ahmad v. State of U.P. [(1955) 1 SCR 707, 718] . Similarly the right to form a corporation is in U.S.A. a "franchise" or a "privilege" which can be withdrawn. To apply the analogy of Banks in U.S.A. to those in India or the mode of exercise by and extent of the powers of a Controller of Currency or some similar authority will more likely than not lead to erroneous conclusions.*

ii) In the case of ***M.C. Mehta v. Union of India (Shriram - Oleum Gas),*** reported in **(1987) 1 SCC 395** this Hon'ble court held as under:-

> ***29.*** *We were, during the course of arguments, addressed at great length by counsel on both sides on the American doctrine of State action. The learned counsel elaborately traced the evolution of this*

doctrine in its parent country. We are aware that in America since the Fourteenth Amendment is available only against the State, the courts in order to thwart racial discrimination by private parties, devised the theory of State action under which it was held that wherever private activity was aided, facilitated or supported by the State in a significant measure, such activity took the colour of State action and was subject to the Constitutional limitations of the Fourteenth Amendment. This historical context in which the doctrine of State action evolved in the United States is irrelevant for our purpose especially since we have Article 15(2) in our Constitution. But it is the principle behind the doctrine of State aid, control and regulation so impregnating a private activity as to give it the colour of State action that is of interest to us and that also to the limited extent to which it can be Indianized and harmoniously blended with our Constitutional jurisprudence. That we in no way consider ourselves bound by American exposition of Constitutional law is well demonstrated by the fact that in R.D. Shetty [(1979) 3 SCC 489 : AIR 1979 SC 1628 : (1979) 3 SCR 1014] this Court preferred the minority opinion of Douglas, J. in Jackson v. Metropolitan Edison Company [42 L Ed (2d) 477] as against the majority opinion of Rehnquist, J. And again in Air India v. Nergesh Meerza [(1981) 4 SCC 335 : 1981 SCC (L&S) 599 : (1982) 1 SCR 438] this Court whilst preferring the minority view in General Electric Company v. Martha V. Gilbert [50 L Ed (2d) 343] said that the provisions of the American Constitution cannot always be applied to Indian conditions or to the provisions of our Constitution and whilst some of the principles adumbrated by the American decisions may provide a useful guide, close adherence to those principles while applying them to the provisions of our Constitution is not to be favoured, because the social conditions in our country are different.

iii) In the case of ***Automobile (Rajasthan) Transport Ltd. v. State of Rajasthan,*** reported in **(1963) 1 SCR 491** this Hon'ble court held as under:-

8. *So far we have set out the factual and legal background against which the problem before us has to be solved. We must now say a few words regarding the historical background. It is necessary to do this, because extensive references have been made to Australian and American decisions, Australian decisions with regard to the interpretation of Section 92 of the Australian Constitution and American decisions with regard to the Commerce clause of the American Constitution. This Court pointed out in the Atiabari Tea Co. case [(1961) 1 SCR 809] that it would not be always safe to rely upon the American or Australian decisions in interpreting the provisions of our Constitution. Valuable as those decisions might be in showing how the problem of freedom of trade, commerce and intercourse was dealt with in other federal constitutions,* ***the provisions of our Constitution must be interpreted against the historical background in which our Constitution was made; the background of problems which the Constitution-makers tried to solve according to the***

genius of the Indian people whom the Constitution-makers represented in the Constituent Assembly. *The first thing to be noticed in this connection is that the Constitution-makers were not writing on a clean slate. They had the Government of India Act, 1935 and they also had the administrative set up which that Act envisaged. India then consisted of various administrative units known as Provinces, each with its own administrative set up. There were differences of language, religion etc. Some of the Provinces were economically more developed than the others. Even inside the same Province, there were under developed, developed and highly developed areas from the point of view of industries, communications etc. The problem of economic integration with which the Constitution-makers were faced was a problem with many facets.*

iv) In the case of ***State of Bihar v. Union of India,*** reported in **(1970) 1 SCC 67** this Hon'ble court held as under:-

13. *Our attention was drawn to some provisions of the American Constitution and of the Constitution Act of Australia and several decisions bearing on the interpretation of provisions which are some what similar to Article 131. But as the similarity is only limited, we do not propose to examine either the provisions referred to or the decisions to which our attention was drawn.* ***In interpreting our Constitution we must not be guided by decisions which do not bear upon provisions identical with those in our Constitution.***

v) In the case of ***Ashoka Kumar Thakur v. Union of India,*** reported in **(2008) 6 SCC 1** this Hon'ble court held as under:-

188. At the outset, it must be stated that the decisions of the United States Supreme Court were not applied in the Indian context as it was felt that the structure of the provisions under the two Constitutions and the social conditions as well as other factors are widely different in both the countries*. Reference may be made to Bhikaji Narain Dhakras v. State of M.P. [AIR 1955 SC 781 : (1955) 2 SCR 589] and A.S. Krishna v. State of Madras [AIR 1957 SC 297 : 1957 SCR 399]* ***wherein this Court specifically held that the due process clause in the Constitution of the United States of America is not applicable to India.*** *While considering the scope and applicability of Article 19(1)(g) in Kameshwar Prasad v. State of Bihar [AIR 1962 SC 1166 : 1962 Supp (3) SCR 369] it was observed: (AIR p. 1169, para 8)*

> *"8. As regards these decisions of the American courts, it should be borne in mind that though the First Amendment to the Constitution of the United States reading 'Congress shall make no law ... abridging the freedom of speech ...' appears*

to confer no power on the Congress to impose any restriction on the exercise of the guaranteed right, still it has always been understood that the freedom guaranteed is subject to the police power—the scope of which however has not been defined with precision or uniformly."

189. *In Kesavananda Bharati case [(1973) 4 SCC 225 : 1973 Supp SCR 1] also, while considering the extent and scope of the power of amendment under Article 368 of the Constitution of India, the Constitution of the United States of America was extensively referred to and Ray, J., held: (SCC p. 615, para 1108)*

"1108. The American decisions which have been copiously cited before us, were rendered in the context of the history of the struggle against colonialism of the American people, sovereignty of several States which came together to form a Confederation, the strains and pressures which induced them to frame a Constitution for a Federal Government and the underlying concepts of law and judicial approach over a period of nearly 200 years, cannot be used to persuade this Court to apply their approach in determining the cases arising under our Constitution."

190. *It may also be noticed that there are structural differences in the Constitution of India and the Constitution of the United States of America. Reference may be made to the Fourteenth Amendment to the US Constitution. Some of the relevant portions thereof are as follows:*

"All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges and immunities of citizens of the United States; nor shall any State deprive any person of life, liberty or property without due process of law nor deny to any person within its jurisdiction the equal protection of the laws."

Whereas in India, Articles 14 and 18 are differently structured and contain express provisions for special provision for the advancement of SEBCs, STs and SCs. Moreover, in our Constitution there is a specific provision under the directive principles of State policy in Part IV of the Constitution requiring the State to strive for justice' social, economic and political—and to minimise the inequalities of income and endeavour to eliminate inequalities in status, facilities and opportunities (Article 38). Earlier, there was a view that Articles 16(4) and 15(5) are exceptions to Articles 16(1) and 15(1) respectively. This view was held in GM, Southern Railway v. Rangachari [AIR 1962 SC 36 : (1962) 2 SCR 586] and M.R. Balaji v. State of Mysore [AIR 1963 SC 649 : 1963 Supp (1) SCR 439] .

209. *The aforesaid principles applied by the Supreme Court of the United States of America cannot be applied directly to India as the gamut of affirmative action in India is fully supported by Constitutional provisions and we have not applied the principles of "suspect legislation" and we have been following the doctrine that every legislation passed by Parliament is presumed to be constitutionally valid unless otherwise proved. We have repeatedly held that the American decisions are not strictly applicable to us and the very same principles of strict scrutiny and suspect legislation were sought to be applied and this Court rejected the same in Saurabh Chaudri v. Union of India [(2003) 11 SCC 146] . Speaking for the Bench, V.N. Khare, C.J., said: (SCC p. 164, para 36)*

> *"36. The strict scrutiny test or the intermediate scrutiny test applicable in the United States of America as argued by Shri Salve cannot be applied in this case. Such a test is not applied in Indian courts. In any event, such a test may be applied in a case where a legislation ex facie is found to be unreasonable. Such a test may also be applied in a case where by reason of a statute the life and liberty of a citizen is put in jeopardy. This Court since its inception apart from a few cases where the legislation was found to be ex facie wholly unreasonable proceeded on the doctrine that constitutionality of a statute is to be presumed and the burden to prove contra is on him who asserts the same."*

vi) In the case of ***Pathumma v. State of Kerala,*** reported in **(1978) 2 SCC 1** this Hon'ble court held as under:-

> **23. <u>We have deliberately not referred to the American cases because the conditions in our country are quite different and this Court need not rely on the American Constitution for the purpose of examining the seven freedoms contained in Article 19 because the social conditions and the habits of our people are different.</u>** In this connection, in the case of *Jagmohan Singh* v. *State of U.P.* [(1973) 1 SCC 20, 27 : 1973 SCC (Cri) 169] this Court observed as follows: (SCC p. 27)
>
> > *"So far as we are concerned in this country, we do not have, in our Constitution any provision like the Eighth Amendment nor are we at liberty to apply the test of reasonableness with the freedom with which the Judges of the Supreme Court of America are accustomed to apply 'the due process' clause."*

XIV. Remedy for breach of Common Law right of privacy

61. It is respectfully submitted that the common law right of privacy has been duly protected by various statutes, subject to reasonable restrictions, as detailed above. In future, in case the Hon'ble Constitutional Courts of the country, finds out that on specific fact situation, privacy of individual is not adequately protected, then the Constitutional Court can, on case to case basis, issue relevant guidelines till the competent legislature steps in as done in the case of *Destruction of Public & Private Properties v. State of A.P.*, reported in *(2009) 5 SCC 212* relevant portion of which reads as under:-

> *" **17.** The power of this Court also extends to laying down guidelines. In Union of India v. Assn. for Democratic Reforms [(2002) 5 SCC 294] this Court observed: (SCC p. 309, paras 19-20)*
>
> > *"19. ... it is not possible for this Court to give any directions for amending the Act or the statutory Rules. It is for Parliament to amend the Act and the Rules. It is also established law that no direction can be given, which would be contrary to the Act and the Rules.*
> >
> > *20. However, it is equally settled that in case when the Act or Rules are silent on a particular subject and the authority implementing the same has Constitutional or statutory power to implement it, the Court can necessarily issue directions or orders on the said subject to fill the vacuum or void till the suitable law is enacted."*
>
> ***18.** This Court has issued directions in a large number of cases to meet urgent situations e.g.*
>
> - *Lakshmi Kant Pandey v. Union of India [(1984) 2 SCC 244]*
> - *Vishaka v. State of Rajasthan [(1997) 6 SCC 241 : 1997 SCC (Cri) 932]*
> - *Vineet Narain v. Union of India [(1998) 1 SCC 226 : 1998 SCC (Cri) 307]*
> - *State of W.B. v. Sampat Lal [(1985) 1 SCC 317 : 1985 SCC (Cri) 62]*
> - *K. Veeraswami [K. Veeraswami v. Union of India, (1991) 3 SCC 655 : 1991 SCC (Cri) 734]*
> - *Union Carbide Corpn. v. Union of India [(1991) 4 SCC 584]*
> - *Delhi Judicial Service Assn. v. State of Gujarat [(1991) 4 SCC 406]*
> - *DDA v. Skipper Construction Co. (P) Ltd. [(1996) 4 SCC 622]*
> - *Dinesh Trivedi v. Union of India [(1997) 4 SCC 306] , Common Cause v. Union of India [(1996) 1 SCC 753 : AIR 1996 SC 929]*
> - *Supreme Court Advocates-on-Record Assn. v. Union of India [(1993) 4 SCC 441]"*

62. It is respectfully submitted that while ascertaining the individuals right of privacy against the state action or against an individual/corporate action the Hon'ble courts would be guided by the test of arbitrariness, test of 'reasonable nexus to the purpose sought to be achieved' and the "test of proportionality". It is submitted that the test embodied under Section 8 (j) RTI Act can also be applied for testing as to whether in a given fact situation, an act / conduct or any other aspect of human life is protected by privacy. As per the said test, a person would have right of privacy if there is no overwhelming public interest in disclosure of the said act / conduct or any other aspect of human life and also the said act has no relationship with any public activity or interest, or which would cause unwarranted invasion of the privacy of the individual. As against this if it is in the larger interest of the nation or in overwhelming public interest not to keep specific kind of information private, its disclosure can be permitted in accordance with the law made by the competent legislature.

63. In nutshell, though each of the citizens of India has an inherent right of privacy, its recognition definition and protection can be done by statutes and not as fundamental rights.

****
****