International Journal of Law
ISSN: 2455-2194; Impact Factor: RJIF 5.12
Received: 10-02-2021, Accepted: 28-02-2021, Published: 25-03-2021
www.lawjournals.org
Volume 7, Issue 2, 2021, Page No. 142-152

Consent in privacy laws: Analysis of India's PDPB, ECPA of USA and GDPR of EU

Adv Prashant Mali
PhD, Founder and President, Cyber Law Consulting (Advocates & Attorneys), Mumbai, Maharashtra, India

Abstract
Consent refers to an affirmative action on the part of the individuals indicating their agreement to the use of their personal data by the collectors or processors for the purpose of processing. Consent has been viewed as an expression of a person's autonomy or control, which has the consequence of allowing another person to legally disclaim liability for acts, which have been consented to. Consent has many connotations in various privacy laws, somewhere it tows the line of prevailing international laws and in some laws it gets localized, but largely consent remains individuals' will to share his / her data. This paper analysis the established privacy laws i.e. EU's GDPR and ECPA of USA with long awaited India's proposed Personal Data Protection Bill. The author has been involved in various government consultations on PDPB since 2006.

Keywords: privacy law, data protection law, GDPR, ECPA, consent, data privacy

Introduction

The requirement of a data principal's consent in order for their data to be lawfully processed has assumed imperative levels in the global data privacy debate. Consent has been viewed as an expression of a person's autonomy or control, which has the consequence of allowing another person to legally disclaim liability for acts which have been consented to [1] The notice and consent framework is based on the philosophically significant act of an individual providing consent for certain actions pertaining to her data [2].

Consent refers to an affirmative action on the part of the data principal indicating their agreement to the use of their personal data by the data fiduciary for the purpose of processing. It can be expressed, for example, by ticking a box when visiting a website or implied from the continued use of a website where a clear notice provides that such use would indicate the user's consent.

Consent under the Personal Data Protection Bill, 2018

The Report of B. N. Saikrishna Committee states that obtaining a user's consent implies liability for any harm that is caused to a data principal pursuant to the latter providing consent, as a consequence of such processing.

The Report identifies some key illustrative harms [3], such as:

1. Such personal data is collected which are not those reasonably expected by the data principal;
2. Purposes for which personal data sought are not those reasonably expected by the data principal;
3. Disclosure and sharing of personal data is allowed with such persons and in such manner not reasonably expected by the data principal.

The Personal Data Protection Bill, 2018 *(hereinafter proposed law)* enumerates its requirements for consent under Chapters III-V, VI and VIII. Section 12 provides that "personal data may be processed on the basis of the consent of the data principal, given no later than at the commencement of the processing". [4] In contrast, the EU-GDPR does not explicitly mention that consent be given at the commencement of processing. Further, the section stipulates certain conditions in order for consent to be valid, such as, it must be "free, informed, specific, clear and capable of being withdrawn" [5].

The section further elaborates on the content of each of these requirements, for example, consent would be considered 'specific' "having regard to whether the data principal can determine the scope of consent in respect of the purposes of processing" [6]. While the expression of these requirements is fairly straightforward in the letter of the Bill, questions regarding their interpretation are bound to arise. As an example, Section 12 states that for consent to be valid, it has to be 'clear' with regard to whether it is indicated through an affirmative action that is meaningful in a given context. The expression 'meaningful' has not been explained, however, and would be open to interpretation. While a data fiduciary would argue for a liberal interpretation, data privacy activists would argue for a stricter approach. Similarly, 'free' consent as provided by the section refers to the meaning conferred on it by provisions of the Contract Act, 1872 [7], that is, consent which is not caused by coercion, undue influence, fraud, misrepresentation or mistake. The interpretation of free consent under the proposed law, therefore, will be shaped by the jurisprudence of 'free consent' under the law of contract. Does a data fiduciary's power to decide whether or not to provide services based on a user's consent preferences constitute 'undue influence'? Practical considerations emerge in the application of principles of contract to the law of data privacy.

It has been prescribed that the data fiduciary shall not make the provision or the quality of any goods or services, the performance of contract, or enjoyment of legal right conditional on consent to processing of any personal data not necessary for that purpose [8] The proposed law does not mention what constitutes 'necessity for that purpose', leaving open much room for interpretation.

The jurisprudence of 'free consent' has largely evolved through precedents under the Indian Contract Act, 1872.

Mutual consent, which should also be a free consent, as

defined in Section 13 and 14 of the Act, is the sine qua non of a valid agreement. One of the essential elements which go to constitute a free consent is that a thing is understood in the same sense by a party as is understood by the other party. It may often be that the parties may realise, after having entered into the agreement or after having signed the contract, that one of the matters which was essential to the agreement, was not understood by them in the same sense and that both of them were carrying totally different impressions of that matter at the time of entering into the agreement or executing the document. On such realisation, it can be legitimately said that the agreement was "discovered to be void". The agreement in such a case would be void from its inception, though discovered to be so at a much later stage [9].

A consent induced by false representation may not be free, but it can nevertheless be real, and ordinarily the effect of fraud or misrepresentation is to render a transaction voidable only and not void [10].

In *Sanjay Dhande & Ors. v. ICICI Bank, Vodafone India Ltd. & Anr* [11], it was observed that while the customers are expected to use their discretion to secure their net banking /mobile banking IDs and passwords, the onus of securing customer's data is on the banks *(and similarly with)* telecommunication companies. In this case, the complainant was defrauded of around Rs. 19 Lakhs as his service provider Vodafone issued a duplicate SIM card without his consent to unscrupulous persons, who then used his number to receive bank OTPs for fraudulent transactions.

It was observed that when a citizen applies for obtaining a SIM card, he provides a battery of information which is personal and sensitive in nature. He reposes his faith and trust in the company that his details and data would not be shared with third parties. It is not hard to realize that such information, if falling in wrong hands, can be misused. A SIM card is a veritable key to person's sensitive financial and personal information. Realizing this, there are clear guidelines issued by the DOT regarding the issuance of SIM cards. The IT Act also intends to ensure that electronic personal and sensitive data is kept secured and reasonable measures are used to maintain its confidentiality and integrity. It is extremely crucial that Telecom companies actively follow strict security procedures while issuing SIM cards. By not implementing security procedures, Vodafone is jeopardizing the sensitive and personal data of all its customers.

Consent under the EU-GDPR

Consent provisions under the EU-GDPR are more comprehensive than in the proposed law. Along with providing a detailed explanation of what constitutes consent in the Articles, the Recitals further elaborate by illustration possible situations how valid consent may be given.

The definition clause of the GDPR explains 'consent' as any "freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". [12] In contrast with the proposed law, therefore, the EU-GDPR defines consent in the definition clause itself.

Certain conditions have been prescribed for 'consent', *viz*.: "the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data". [13] If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language" [14] When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract" [15].

Article 7, therefore, elaborates on the definition of consent, by dwelling upon what constitutes consent that is 'freely given', besides stating the manner in which the request for consent shall be presented. This is more elaborate than the proposed law, where the question of 'undue influence' remains open, as discussed.

Consent should be freely given

Recital 32 elaborates that a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them.

Further, Recital 43 provides that in order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.

Recital 42 states that consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

Therefore, the meaning of 'clear affirmative action' in the definition of consent is elaborated upon in reasonable detail, along with illustrations as to what may or may not constitute consent. Additionally, there is an attempt to balance the interests of the data subject against those of the data controller where there exists a clear imbalance, with particular mention to public authorities as the controller. 'Freely given' consent is also explained to mean 'genuine' or 'free choice' and an ability to 'refuse or withdraw consent without detriment'. This comprehensively tightens the meaning of freely given consent, in effect empowering the data subject against unfair consent policies of data controllers. Similar to the proposed law, it is provided that there must be separate consent for separate data processing

operations as well as that the performance of a contract (including the provision of a service) should not be dependent on consent where such consent is not necessary for such purpose. Therefore, what constitutes 'necessary for such purpose' is ambiguous, leaving wide room for data controllers to operate.

Written declaration for consent

Recital 42 states that in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. The consent declaration should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended.

This Recital elaborates on consent in the context of written declaration and adds more to the definition by including data subject's awareness as a factor. Importantly, it adds that a consent declaration should not contain unfair terms. The provision seeks to empower the data subject but falls short of explaining the scope of the term 'unfair terms'. Seen as a fair practice measure, however, it may be inferred that the adjudicators will tend towards a liberal interpretation that favours the data subject. Importantly, the data subjects' awareness of the 'identity of the controller' and 'purpose of processing' have been added as factors.

It is seen, therefore, that the Recitals explain to a fair degree the content of some of the terms used in the definition of consent. In contrast, the proposed law's explanation of the terms used to the meaning of 'consent' is limited, leaving open much room for ambiguity.

While being one of the more well-known legal bases for processing personal data, consent is only one of six bases mentioned in the General Data Protection Regulation (GDPR). The others are: contract, legal obligations, vital interests of the data subject, public interest and legitimate interest as stated in Article 6(1) GDPR [16].

Therefore, in spite of the consent provisions in the GDPR being significantly more comprehensive than the proposed law, it is not the only legal basis for processing of personal data, in turn diluting the consent provision to some degree.

The first major crackdown against a U.S. tech giant and the most recent reported violation of the EU-GDPR was in January 2019, with the French regulator CNIL fining Google nearly $57 million for failure to adequtely disclose to its users the collection of their personal information and its operations on their data. Google was also charged with failing to properly obtain users' consent for showing them personalized ads. The CNIL said that "the infringements observed deprive the users of essential guarantees regarding processing operations that can reveal important parts of their private life since they are based on a huge amount of data, a wide variety of services and almost unlimited possible combinations" [17]. It was observed by CNIL that Google erred on both – giving users a complete and clear picture of their data collection, and providing simple tools for users to provide consent for their data to be processed. Google in its turn responded that people expect high standards of transparency and control from them and they were deeply committed to meeting those expectations and the consent requirements of the GDPR, adding that they were determining next steps.

Consent under US Data Privacy Laws

The United States largely has a patchwork system of sectorial and state legislations that cover different sectors and vary greatly across states. The regulatory framework lacks consolidation and the multiplicity of legislation has complicated the enforcement of data privacy rights of individuals.

The following are some sectorial legislations in the US that address data privacy:

- The Federal Trade Commission Act (15 U.S.C. §1681) is a consumer protection law that prohibits trade practices that are deceptive or unfair and has been applied to both online and offline privacy and data protection policies. With the exception of certain telecommunications, transportation and financial companies, the Act applies to most individuals and companies doing business in the US.
- Children's Online Privacy Protection Act (15 U.S.C. §§6501-6506) is aimed at protecting children online by regulating the information collected from children online.
- The Health Insurance Portability and Accountability Act (42 U.S.C. §1301) is of application to pharmacies, healthcare providers, data processors and other entities that deal with medical information.
- The Electronic Communications Privacy Act (18 U.S.C. §2510) targets 'snooping', that is, the interception of electronically transmitted communication.
- The Financial Services Modernization Act (15 U.S.C. §§6801-6827) applies to financial institutions and other businesses providing financial products and services, such as banks, insurance companies and securities firms and is aimed at regulating the disclosure, collection and use of financial information.
- The Fair Credit Reporting Act (15 U.S.C. §1681) is targeted at consumer reporting agencies – both – users and providers of reports.
- The California Consumer Privacy Act, 2018 passed by the State of California is the most extensive of all privacy laws in the US. The bill contextualises the need for protection of data privacy in terms of the rise of big data and the omnipresent and omnipotent role of data in the everyday lives of people. With the effective date (1st January, 2020) fast approaching, businesses are scrambling to bring their practices in line with the new law.

For the purpose of this paper, we will analyse consent provisions under the Electronic Communications Privacy Act (ECPA) and the Health Insurance Portability and Accountability Act (HIPPA).

Consent under ECPA

The ECPA has three titles [18]

Title I, known as the Wiretap Act, prohibits the intentional actual or attempted interception, use or disclosure of any interception or endeavor to intercept any wire, oral, or electronic communication.

Title II, known as the Stored Communications Act (SCA), protects the privacy of files stored with service providers and records held about the subscriber by service providers, such as subscriber name, billing records, or IP addresses.

Title III addresses pen register and trap and trace devices.

Title I – The Wiretap Act

The Wiretap Act allows "a person acting under the colour of law" to intercept a wire, oral or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception [19]. Further, the Act also allows a person not acting under the colour of law to intercept such communication where such person is a "party to the communication" or where "one of the parties to the communication has given prior consent to such interception, except, where such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State" [20].

The Act thus allows interception of electronic communication by individuals "acting under colour of law" and those outside the colour of law under certain circumstances. It is noteworthy that the act does not name specific entities such as, say, government officials or law enforcement agencies but instead goes for a much wider scope by mentioning persons "acting under the colour of law", which may be extended to include multiple functionaries. For such interception to be legal, one of the two conditions is necessary, i.e. the person must be a party to the communication; or, one of the parties to the communication must have given prior consent to such interception. Therefore, 'consent' of only one of the parties to the communication would suffice for such interception to be legal. Furthermore, such consent is not even necessary where such person is a party to the communication.

The Act also provides that a person or entity providing electronic communication service to the public may divulge the contents of any such communication on the fulfillment of any of the conditions provided. These include: with the lawful consent of the originator or any addressee or intended recipient of such communication; to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency; or, as otherwise provided in the Act.

It is seen again that 'consent' does not attain primacy in questions of disclosure of intercepted personal communications.

Title II – The Stored Communications Act

The SCA applies to persons or entities providing electronic communication service or remote computing services to the public, which it terms as 'providers'.

It allows for the disclosure of the contents of a communication by providers under three circumstances, i.e., "if such disclosure is to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient"; "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service"; or, as otherwise authorised in the Act [21]

Similarly, it allows for the disclosure of a record or other information pertaining to or customer of such service, excluding the contents, under three circumstances, i.e., "with the lawful consent of the customer or subscriber"; "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service"; as otherwise authorised to the government [22].

Therefore, in case of disclosure of the contents of a communication, the 'consent' of the originator or addressee or intended recipient, and, in the case of disclosure of customer or service record, the 'consent' of customer or subscriber, will deem such disclosures lawful. In both scenarios, however, consent is one of the circumstances and the disclosure will remain lawful even if any one of the other conditions provided are fulfilled.

Consent under HIPPA

The Act covers 'individually identifiable health information', which it defines as "any information, including demographic information collected from an individual, that: is created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and — identifies the individual; or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual" [23].

The Privacy Rule was issued by the U.S. Department of Health and Human Services to fulfill the requirement under HIPAA.

'Protected health information' (PHI) under Privacy Rules means "individually identifiable health information that is transmitted by electronic media; or maintained in electronic media; or transmitted or maintained in any other form or medium" [24].

The applicability of the Act extends to 'covered entities', defined as: "a health plan; a health care clearinghouse; or a health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter" [25].

The Act regulates 'use' and 'disclosure' of PHI. 'Use' means "the sharing, employment, application, utilisation, examination, or analysis of such information within an entity that maintains such information" [26]. 'Disclosure' means "the release, transfer, provision of, access to, or divulging in any other manner, of information outside the entity holding the information" [27].

The HIPAA and Privacy Rule categorizes the validation of the individual (for PHI disclosure) into: consent and authorization.

Consent

The Privacy Rules provides that a covered entity may obtain consent of the individual to use or disclose protected health information to carry out treatment, payment, or health care operations [28]. Thus, the consent of the individual is not required, but permitted.

Authorization

An authorization is a detailed document that gives covered entities permission to use protected health information for specified purposes, which are generally other than treatment, payment, or health care operations, or to disclose protected health information to a third party specified by the individual [29].

The Privacy Rule provides certain conditions that must be fulfilled in order for an authorization to be valid. Thus, "a valid authorization must contain at least the following core elements [30]:

1. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;
2. The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;
3. The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure;
4. A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose;
5. An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research repository;
6. Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided."

In addition to the core elements, "the authorization must contain statements adequate to place the individual on notice of all of the following [31]:

1. The individual's right to revoke the authorization in writing;
2. The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization;
3. The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected by this subpart.
4. The authorization must be written in plain language;
5. If a covered entity seeks an authorization from an individual for a use or disclosure of protected health information, the covered entity must provide the individual with a copy of the signed authorization."

The Privacy Rule states that "except as otherwise permitted or required, a covered entity may not use or disclose protected health information without an authorization that is valid" [32].

An authorization is required under the following circumstances [33]:

- For any use or disclosure of psychotherapy notes; except,

1. Use by the originator of the psychotherapy notes for treatment;
2. Use or disclosure by the covered entity for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling;
3. Use or disclosure by the covered entity to defend itself in a legal action or other proceeding brought by the individual;

- For any use or disclosure of protected health information for marketing, except if the communication is in the form of,

1. A face-to-face communication made by a covered entity to an individual; or,
2. A promotional gift of nominal value provided by the covered entity

- For any disclosure of protected health information which is a sale of protected health information

Further, there are certain circumstances under which a covered entity may use or disclose protected health information, provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the use or disclosure [34].

Finally, A covered entity may use or disclose protected health information without the written authorization of the individual, or the opportunity for the individual to agree or object in the following situations [35]:

- Uses and disclosures required by law
- Uses and disclosures for public health activities
- Disclosures about victims of abuse, neglect or domestic violence
- Uses and disclosures for health oversight activities
- Disclosures for judicial and administrative proceedings
- Disclosures for law enforcement purposes
- Uses and disclosures about decedents
- Uses and disclosures for cadaveric organ, eye or tissue donation purpose
- Uses and disclosures for research purposes
- Uses and disclosures to avert a serious threat to health or safety
- Uses and disclosures for specialized government functions
- Disclosures for workers' compensation

The HIPAA read with the Privacy Rule, thus, provides an in-depth and comprehensive set of rules and conditions to be followed for use and disclosure of PHI. It is significantly more complex than the provisions relating to "sensitive personal data" under the Indian proposed law, the EU-GDPR, and even ECPA.

Consent Fatigue

Comprehensive consent provisions would mean that data acquisition tick-boxes should not be pre-checked, especially where sensitive personal data is being dealt with by the organisation.

Comprehensive consent requirements such as specificity and informed consent mean that users might be faced with consent demands that are potentially overwhelming. Pereira *et al* have argued that repetitive consent acquisition points could lead to consent fatigue [35]. The ordinary user, faced with a flurry of consent requests, may not have the time or inclination to respond to or keep track of all of them. Individuals with special needs, children and the elderly might face this to an even greater degree.

This concern is also addressed in the GDPR in Recital 32, which states that if the data subject's consent is to be given

following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

If a website's returning customers are bombarded with consent requests at each stage of their online experience, frustration can continue to build, until there is a risk of losing their business to competitors. It is crucial for businesses to understand what their customers have consented to in order to avoid repetitive consent requests. This is where good data consent management platforms are crucial [36].

Consent Management System

The GDPR states that "where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data" [37]. Similarly, the proposed law states that "the data fiduciary shall bear the burden of proof to establish that consent has been given by the data principal for processing of personal data" [38]. Under the GDPR, this requirement has translated into companies marketing 'Consent Management Systems'.

A consent management system is designed to capture and manage consent requirements under data protection laws [38]. Since multiple customers are expected to have varying consent preferences with respect to different products and services, consent management systems would enable a data fiduciary to handle all these consent requirements – including, but not limited to – the name of the data principal, the date, type and purpose for which consent was given, along with changes to consent preferences such as modification as well as withdrawal.

Whereas the proposed law mandates data fiduciaries to maintain "accurate and up-to-date records of important operations in the data life-cycle including collection, transfers, and erasure of personal data" [39], it falls short of mandating the maintenance of records for individuals' consent preferences. Thereby, it is left open to the discretion of data fiduciaries to establish mechanisms that evidence the consent of data principals for the processing of their personal data.

The burden of proof upon the data fiduciary to establish valid consent of the data principal can be effectively discharged by the consent management system described above. This system would enable data fiduciaries to evidence informed consent on the part of the data principal in case of changes. Up-to-date logs of consent details along with screens wherever necessary would enable organisations to better manage their consent obligations under the proposed law.

It is recommended that the consent management system be built into the data fiduciary's system in order to best serve the interests of data principal's privacy as well as fulfill the data fiduciary's obligations under 'privacy by design'.

Section 29 of the proposed law provides for 'privacy by design', a list of policies and measures that data fiduciaries shall implement. The provision mandates that managerial, organisational, business practices and technical systems be designed in a manner to "anticipate, identify and avoid harm to the data principal" [40]. It also mandates "the use of certified technology in data processing" [41]; "transparency" [42]; "protection of privacy throughout processing from the point of collection to deletion of personal data" [43] as well as "accounting for the data principal's interest at every stage of processing" [44]. Put simply, privacy by design means nothing more than "data protection through technology design." Behind this is the thought that data protection in data processing procedures is best adhered to when it is already integrated in the technology when created [45].

Consent management systems should be built into the data processing technology instead of being implemented as an end-measure. This would ensure that data principals' consent preferences are prioritised and consent management remains the key aspect in data processing activities.

The legislative effort to strengthen consent provisions falls short on two accounts. Firstly, as explained above, due to the ambiguity of the terms used in explaining the meaning of valid consent. Secondly, due to the non-exclusivity of consent as a prerequisite in the lawful processing of personal data, that is, the proposed law does not limit the processing of personal data to that on the basis of consent only. According to Ss. 13-17, personal data can be processed on grounds such as: State functions, compliance with court or tribunal orders, prompt action in case of medical emergencies and natural disasters, employment reasons as well as other reasonable purposes. These grounds provide comfortable maneuvering space to data fiduciaries, in turn diluting the consent provision.

1. Types of Consent

The consent requirements in the proposed law can be categorized on the basis of the *type of data* and the *age of the data principal.* Whereas Section 12 provides for the processing of personal data based on consent, Section 18 provides for the processing of *sensitive personal data* based on *explicit consent* of the data principal. Further, Section 23 provides for the processing of personal data and sensitive personal data of *children*, carving out a separate category of data principals.

A. Based on Type of Data

Under the Data Protection Bill, 2018

The proposed law creates two categories of consent requirements on the basis of the type of data for the processing of which consent is being sought. Whereas Section 12 provides for processing of personal data based on consent, Section 18 provides for processing of sensitive personal data based on explicit consent. Thus, certain types of data are elevated into the "sensitive" category. The definitions clause explains "sensitive personal data" as "personal data revealing, related to, or constituting, as may be applicable – passwords, financial data, health data, official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe, religious or political belief or affiliation; or any other category of data specified by the Authority" [46].

Section 18 provides that "sensitive personal data may be processed on the basis of explicit consent" [47]. For consent to be explicit, it must be valid as per Section 12, as well as be:

- "Informed, having regard to whether the attention of the data principal has been drawn to purposes for operations in processing that may have significant consequences for the data principal;
- Clear, having regard to whether it is meaningful without recourse to inference from conduct in a context; and
- Specific, having regard to whether the data principal is

> given the choice of separately consenting to the purposes of, operations in, and the use of different categories of sensitive personal data relevant to processing" [48].

Explicit consent, therefore, must be 'informed', in that the data principal must be "provided with information required under Section 8" [49] as well as the attention of the data principal has to be drawn to purposes for operations in Processing having significant consequences for them. The term 'significant consequences', however, is wide and ambiguous and no explanation has been offered in the statute. Consent must further be 'clear' in that it must be meaningful without recourse to inference from conduct – that is – it must be express, not implied. This is different from Section 12, which provides that consent can be both – express and implied. The requirement for explicit consent also adds to the meaning of 'specific' in Section 12; for explicit consent to be specific, the data principal should be given the choice of separately consenting to the purposes, operations and use of different categories of sensitive personal data, in addition to them being able to determine the scope of consent in respect of processing.

In *Rohit Maheshwari v. Vodafone India Limited and Ors.* [50] it was observed that telecom companies are trustees of customers' data and have to be judged on tough standards. A strong signal must be sent to them that they need to protect the privacy of their customers.

In this case, the complainant had alleged that Vodafone had allowed a change of his registered email ID and dispatched e-bills to unknown persons without his consent, amounting to a breach of sensitive personal data. Notably, Vodafone had argued that they had followed all reasonable security checks and that item wise billing details of a customer are not included within sensitive personal data as contemplated under the IT Act and Rules.

It was observed that mobile phone or SIM acrds act as "Master Key" or "Master Password" to a citizen's digital repository. The call detail records or item wise billing details can reveal many sensitive personal information. Call logs to banks, financial institutions, insurance companies, luxury stores etc. can reveal financial information, call records to doctors can reveal medical conditions such as pregnancy, cancer, AIDS, etc. Thus, item wise billing details are definitely a sure shot door to personal sensitive data, hence to be treated as Personal Sensitive Data under IT Act. It was also observed that Vodafone's Privacy Policy is really loaded against the customer, with respect to provisions regarding the extent of information collected, with whom it may be shared, and so on.

Under the EU-GDPR

The differentiation between 'consent' and 'explicit consent' is not as categorical in the GDPR as in the proposed law. Since the provisions for consent itself are fairly comprehensive, the requirement for explicit consent is left to specific categories and uses of personal data.

All consent must involve a specific, informed and unambiguous indication of the individual's wishes. The key difference is likely to be that 'explicit' consent must be affirmed in a clear statement (whether oral or written). Consent that is inferred from someone's actions cannot be explicit consent, however obvious it might be that they consent. Explicit consent must be expressly confirmed in words [51].

Whereas Article 7 and its supporting Recitals detail provisions for consent, explicit consent is required in specific use cases such as international transfers, profiling and automated decision making and for data categorised as sensitive personal data.

- **Sensitive Personal Data**

At the outset, the GDPR prohibits the processing of "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation" [52]. However, this prohibition shall not apply if the data subject has given "explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provides that this prohibition may not be lifted" [53].

Thus, there is a specific prohibition against processing sensitive personal data, which may be lifted in certain circumstances, one of which is explicit consent of the data subject.

- **International Transfers**

Chapter 5 of the GDPR provides for transfer of personal data to a third country or international organisation under certain specific situations. Such transfers could be effected on the basis of an 'adequacy decision', that is, where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an "adequate level of protection" [54]. Where the adequacy decision is absent, such transfer could be effected where the controller or processor has provided 'appropriate safeguards', and on condition that "enforceable data subject rights and effective legal remedies for data subjects are available" [55].

However, in the absence of both – adequacy decision and appropriate safeguards – a transfer of personal data to a third country or international organisation shall take place only on one of the conditions mentioned, which include, among others, the explicit consent of the data subject. Thus, the data subject should have explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards [56].

- **Profiling and Automated Decision Making**

The GDPR guarantees data subjects the right not to be subject to a decision based solely on automatic processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her [57]. However, it provides an exception where such decision is based on the data subject's explicit consent [58].

B. Based on Age of Data Principal

Under the Data Protection Bill, 2018

The definition clause explains "child" as a data principal below the age of eighteen years [59]. The proposed law carves out a separate provision for the processing of personal data and sensitive personal data of children. Measures such as age verification and parental consent have

been prescribed in order to ensure that the processing of personal data of children is done in a manner that protects and advances the rights and best interests of the child. Therefore, the provisions with respect to children's data apply in addition to the provisions with respect to personal data and sensitive personal data mentioned in the previous sections.

2. Consent of Children

Under the Data Protection Bill, 2018

Section 23 provides that "every data fiduciary shall process personal data of children in a manner that protects and advances the rights and best interests of the child" [60]. "Appropriate mechanisms for age verification and parental consent shall be incorporated by data fiduciaries in order to process personal data of children" [61]. "Appropriateness of an age verification mechanism incorporated by a data fiduciary shall be determined on the basis of: volume of personal data processed; proportion of such personal data likely to be that of children; possibility of harm to children arising out of processing of personal data; and such other factors to be specified" [62].

Further, there is a provision for the Authority to notify guardian data fiduciaries, that is, "data fiduciaries responsible for operating commercial websites or online services directed at children; or who process large volumes of personal data of children" [63]. The Section places restrictions upon guardian data fiduciaries in the interest of children's safety and privacy. Therefore, "guardian data fiduciaries shall be barred from profiling, tracking, or behavioral monitoring of, or targeted advertising directed at, children and undertaking any other processing of personal data that can cause significant harm to the child" [64]. For data fiduciaries offering "counseling" or "child protection services to a child", the above restrictions "may apply in modified form" [65]. Further, where a guardian data fiduciary exclusively provides counseling or child protection services to a child, such guardian data fiduciary will not be required to obtain parental consent.

The Section, therefore, limits certain data processing activities of guardian data fiduciaries, along with providing for age verification and parental consent mechanisms. However, there is ambiguity on what these mechanisms should mandatorily contain and the desired objectives. Further, only guardian data fiduciaries have been prohibited from certain potentially harmful data processing activities, but no such bar has been placed on data fiduciaries operating websites targeted at all age groups, that may also be used by children. Notably, there is no complete bar on the processing of personal data and even sensitive personal data of children, and such processing has been left subject to parental consent.

Under the EU-GDPR

Article 8 contains the conditions applicable to child's consent in relation to information society services. The offer of information society services can be made directly to a child, including the lawful processing of their personal data, when the child is "at least 16 years old" [66]. This is to apply when the data subject has given consent to the "processing of his or her personal data for one or more specific purposes" [67].

Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. "Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years" [68]. The controller is mandated to make reasonable efforts to verify in such cases that consent is "given or authorised by the holder of parental responsibility over the child", taking into consideration available technology [69].

Recital 38 duly acknowledges the need for special protection required by children with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. "The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child" [70].

Thus, the GDPR categorises children as those at least 16 years old and those below 16 years, but not below 13 years old. Children who are at least 16 years old may consent to the processing of their personal data for one or more specific purposes. However, consent is required to be given or authorised by the holder of parental responsibility for children below the age of 16 years. It places responsibility upon the controller to make reasonable efforts to verify that such consent is given or authorised by the appropriate person, taking into consideration the existing technology. Thus, there is a positive burden placed on the data controller to ensure lawful processing of children's data.

3. Withdrawal of Consent

Under Data Protection Bill

The proposed law makes the capability of consent to be withdrawn a precondition for consent to be valid. Section 12 states that along with being free, specific, informed, and clear, consent must also be "capable of being withdrawn", in order to be valid [71]. The capability of consent to be withdrawn has thus been constructed into the meaning of consent itself, thereby making it an indispensible part of data processing on the basis of consent.

Further, the Section provides that where "the data principal withdraws consent for the processing of any personal data necessary for the performance of a contract to which the data principal is a party, all legal consequences for the effects of such withdrawal shall be borne by the data principal" [72]. It does not clarify, however, what legal consequences might flow from such withdrawal, and whether such legal consequences would in normal course emerge for the data fiduciary or the data principal. The phrase 'all legal consequences' is of very broad scope, making it a concern for the data principal in question about the extent of liability imposed on him for withdrawal of consent [73].

Sections 39 and 53 of the Indian Contract Act have been referenced in order to explain the above provision. However, a direct reference to these sections of the Contract Act in the Data Protection Bill may have played a better role in limiting the effects of withdrawal of consent for necessary data by the data principal. Alternately, a specific mention that the data fiduciary will have the right to refuse performance of the contract which depends on the data that was withdrawn, or his entitlement to compensation for losses incurred, would have served the same purpose [74].

Notice

The proposed law also makes the notice of the right of the data principal to withdrawal consent imperative. It mandates the data fiduciary to provide the data principal with "information about the right of the data principal to withdraw consent, and the procedure for such withdrawal, if the personal data is intended to be processed on the basis of consent" [75]. It is mandated that such information be provided by the data fiduciary "no later than at the time of collection of the personal data or, if the data is not collected from the data principal, as soon as is reasonably practicable" [76]. It is seen that this provision adds meaning to the requirement for valid consent to be capable of being withdrawn, as provided under Section 12.

Right to Be Forgotten

Section 27 enunciates an important right of the data principal, which has come to be known as the touchstone of consent in the data privacy debate, by recognising the data principal's 'Right to be Forgotten'. "The data principal shall have the right to restrict or prevent continuing disclosure of personal data by a data fiduciary related to the data principal where such disclosure was made on the basis of consent under section 12 and such consent has since been withdrawn" [77].

However, this provision shall only apply where "the rights and interests of the data principal in preventing or restricting the continued disclosure of personal data override the right to freedom of speech and expression and the right to information of any citizen" [78]. This is a wide caveat and leaves the right for a data principal to ensure data destruction subject to the right to freedom of speech and expression and the right to information. There are some guidelines, however, provided in the next subsection. Some of the considerations to be taken into account are: "the sensitivity of the personal data; the scale of disclosure and the degree of accessibility sought to be restricted or prevented; the role of the data principal in public life; the relevance of the personal data to the public; and the nature of the disclosure and of the activities of the data fiduciary, particularly whether the data fiduciary systematically facilitates access to personal data and whether the activities would be significantly impeded if disclosures of the relevant nature were to be restricted or prevented" [79]. Therefore, it is observed that the right to be forgotten is not balanced strongly towards data-destruction, making the latter subject to various considerations. It can be seen that public interest has taken precedence over the interest of the individual data principal.

Data Destruction

The definition clause explains "processing" in relation to personal data, as "an operation or set of operations performed on personal data, and may include operations such as, among others, erasure or destruction" [80]. Thus, erasure or destruction of personal data are both included in the meaning of data processing activities.

It is noteworthy that whereas the proposed law recognizes the data principals' 'Right to be Forgotten', it does not mention the removal, destruction, or erasure of data as inherent to this right. Instead, the section recognizes the right of the data principal to *restrict* or *prevent continuing disclosure of personal data*, falling just short of complete removal of personal data. It remains to be understood what mechanisms would be put in place in order to allow for data principals to exercise this right, and whether the right to be forgotten without a right to data erasure will truly serve the interests of data privacy.

Thus, the data fiduciary shall not have an obligation to erase or destroy the personal data of the data principal upon the withdrawal of consent to processing by the data principal.

Under EU-GDPR

The GDPR recognizes the right of the data subject to withdraw his or her consent at any time. Further, it is provided that "the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent" [81].

Thus, the GDPR encompasses the provision for withdrawal of consent and its various conditions under one Article, including 'notice' and ease of withdrawal of consent.

Further, Recital 42 expands the conception of 'freely given' consent by adding the requirement that the data subject must be able to refuse or withdraw consent without detriment.

Right to Be Forgotten

Article 17 specifically provides for the 'Right to Erasure', which it also terms as the 'Right to Be Forgotten'. "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay, where the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing" [82].

Thus, the GDPR effectively recognizes the data subjects' 'right to erasure', terming it alongside the 'right to be forgotten'. This title of the Article is relevant as it recognizes the right to erasure as inherent to the right to be forgotten. It is significantly stronger than the right to be forgotten in the proposed law, wherein the right is limited to restricting or preventing the continued disclosure of personal data, but not its complete erasure or destruction.

Recital 65 explains the scope of the right to erasure and illustrates situations that highlight the need for this right. A data subject should have the right to have his or her personal data erased and no longer processed where a data subject has withdrawn his or her consent. That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.

Therefore, whereas the right to erasure of data in case of withdrawal of consent is recognized, it is balanced against needs of public interest and legal obligations.

Under US Laws

HIPAA

An individual may revoke an authorization provided under this section at any time, provided that the revocation is in writing, except to the extent that: the covered entity has taken action in reliance thereon; or if the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy or the policy itself.

Thus, where action has been taken in pursuance of the authorization, an individual cannot withdraw his or her authorization. This is in contrast to the proposed law and the EU-GDPR, which contain provisions for withdrawal of consent irrespective of whether action has been taken in pursuance.

Conclusion

With burgeoning big data and new technologies getting intrinsically linked to people's everyday lives, tough data privacy measures are an absolute must. Whereas the B.N. Saikrishna Committee Report reinforces the need for comprehensive consent framework, the proposed law leaves much to be desired. The EU-GDPR, on the other hand, has gone a long way to tighten the bolt around individual consent and provides a battery of requirements that must be adhered to by data aggregators in order to comply with its consent requirements. The EU has also set an example in enforcement by going after tech giants in order to ensure compliance to consent provisions. The United States, however, still lacks a federal data privacy law with only a patchwork approach that is to be seen. Its own sectorial and state legislations such as ECPA, HIPAA and the California Consumer Privacy Act could lead the way for a consolidated legislation at the federal level.

It is also important to remember that in the same way as a standard can stifle innovation, similarly the law can stifle businesses. The impact of laws on businesses is only observed over a period of time. It is also true to say that the absence of law allows leapfrogging, so even though consent is written in black and white all over the law, the understanding of consent and its implementation will require jurisprudence around consent to evolve. Take, for example, a user who consents to the 'collection and processing of her personal data' via a single check-box. Ticking a single box on the user's end might translate into consent equivalent to ticking 20 boxes for various processing activities by the business.

Kate O' Neill, author of Tech Humanist says that it's simply worth becoming more mindful of how our data can be used. We don't need to be wary of everything; we just need to think critically, and learn more about the potential our data has at scale. We're all still learning [83].

It must be noted that the game of consent to comply with these laws is intertwined with existing and prevailing technology. Consent in written or through oral communication simplifies things, but when it comes to compliance of consent by technologies, there are many unknown unknowns. Therefore, only time would reveal the fate of law related to consent, globally and in India.

References

1. Adam Moore, Toward Informational Privacy Rights, 44 San Diego Law Review (2007) at p. 812; Anita L. Allen, Nature of Consent in The Ethics of Consent-Theory and Practice (Alan Wertheimer and Franklin Miller (eds.), Oxford University Press, 2009) at p. 4.
2. Ryan M. Calo, Against Notice Skepticism in Privacy (and Elsewhere), 87(3) Notre Dame Law Review (2012) at p. 1049
3. B.N. Saikrishna Report, p. 34
4. Section 12(1), Personal Data Protection Bill, 2018
5. Section 12(2), Personal Data Protection Bill, 2018
6. Section 12(2)(c), Personal Data Protection Bill, 2018
7. Section 12(2)(a), Personal Data Protection Bill, 2018
8. Section 12(3), Personal Data Protection Bill, 2018
9. *Sri Tarsem Singh v. Sukhminder Singh AIR 1998 SC 1400*
10. *Central National Bank Ltd v. United Industrial Bank Ltd. 1954 AIR 181*
11. Complaint No. 30 of 2013, Order Dated: 16th Jan., 2014
12. Article 4(11), EU-GDPR
13. Article 7(1), EU-GDPR
14. Article 7(2), EU-GDPR
15. Article 7(4), EU-GDPR
16. Intersoft Consulting, GDPR – Consent, https://gdpr-info.eu/issues/consent/
17. France fines Google nearly $57 Million for First Major Violation of New European Privacy Regime - https://www.washingtonpost.com/world/europe/france-fines-google-nearly-57-million-for-first-major-violation-of-new-european-privacy-regime/2019/01/21/89e7ee08-1d8f-11e9-a759-2b8541bbbe20_story.html?noredirect=on&utm_term=.efc63c1af210
18. US Department of Justice, Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22, https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285
19. The Wiretap Act, 1986, §2511(2)(c)
20. The Wiretap Act, 1986, § 2511(2)(d)
21. The SCA, 1986, § 2702(b)
22. The SCA, 1986, § 2702(c)
23. The HIPAA, 1996, § 1171(6)
24. 45 CFR § 160.103
25. 45 CFR § 160.103
26. 45 CFR § 160.103
27. 45 CFR § 160.103
28. 45 CFR § 164.506(b)(1)
29. What is the difference between "consent" and "authorization" under the HIPAA Privacy Rule? – US Department of Health and Human Services
30. 45 CFR § 164.508(c)(1)
31. 45 CFR § 164.508(c)(2)
32. 45 CFR § 164.508(a)(1)
33. 45 CFR § 164.508(a)
34. 45 CFR § 164.510
35. 45 CFR § 164.512
36. European Commission, JRC Scientific and Policy Reports, Agency in the Internet of Things, Pereira *et al*. (2013)
37. How to Avoid Consent Fatigue – Trunomi, 12th November, 2018, Benjamin Ellis, https://www.trunomi.com/consent-fatigue/
38. Article 7, General Data Protection Regulation
39. Section 12(4), Data Protection Bill, 2018
40. IBM Knowledge Centre, Overview of Consent Management, https://www.ibm.com/support/knowledgecenter/en/SS

WSR9_11.6.0/com.ibm.mdmhs.overview.doc/consentmanagementoverview.html
41. Section 34, Personal Data Protection Bill, 2018
42. Section 29(a), Personal Data Protection Bill, 2018
43. Section 29(c), Personal Data Protection Bill, 2018
44. Section 29(f), Personal Data Protection Bill, 2018
45. Section 29(e), Personal Data Protection Bill, 2018
46. Section 29(g), Personal Data Protection Bill, 2018
47. Intersoft Consulting, GDPR – Privacy by Design, https://gdpr-info.eu/issues/privacy-by-design/
48. Section 3(35), Personal Data Protection Bill, 2018
49. Section 18(1), Personal Data Protection Bill, 2018
50. Section 18(2), Personal Data Protection Bill, 2018
51. Section 12(1)(b), Personal Data Protection Bill, 2018
52. Complaint Case No. 16 of 2013, Order Dated: 4th Feb., 2014
53. Information Commissioner's Office, 'What is valid consent'? - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/
54. Article 9(1), EU-GDPR
55. Article 9(2)(a)
56. Article 45, EU-GDPR
57. Article 46, EU-GDPR
58. Article 49, EU-GDPR
59. Article 22(1), EU-GDPR
60. Article 22(2)(c), EU-GDPR
61. Section 3(9), Personal Data Protection Bill, 2018
62. Section 23(1), Personal Data Protection Bill, 2018
63. Section 23(2), Personal Data Protection Bill, 2018
64. Section 23(3), Personal Data Protection Bill, 2018
65. Section 23(4), Personal Data Protection Bill, 2018
66. Section 23(5), Personal Data Protection Bill, 2018
67. Section 23(6), Personal Data Protection Bill, 2018
68. Article 8(1), EU-GDPR
69. Article 6(1)(a), EU-GDPR
70. Article 8(1), EU-GDPR
71. Article 8(2), EU-GDPR
72. Recital 38, EU-GDPR
73. Section 12(2)(e), Personal Data Protection Bill, 2018
74. Section 12(5), Personal Data Protection Bill, 2018
75. Data Protection Bill Series: Standard of Consent, Asheeta Regidi, https://www.firstpost.com/tech/news-analysis/data-protection-bill-series-standard-of-consent-and-processing-of-data-4886981.html
76. Id.
77. Section 8(1)(d), Personal Data Protection Bill, 2018
78. Section 8(1), Personal Data Protection Bill, 2018
79. Section 27(1)(d), Personal Data Protection Bill, 2018
80. Section 27(2), Personal Data Protection Bill, 2018
81. Section 27(3), Personal Data Protection Bill, 2018
82. Section 3(32), Personal Data Protection Bill, 2018
83. Article 7(3), EU-GDPR
84. Article 17(1)(b), EU-GDPR
85. Kate O' Neill – Twitter, https://twitter.com/kateo/status/1084506956658806785