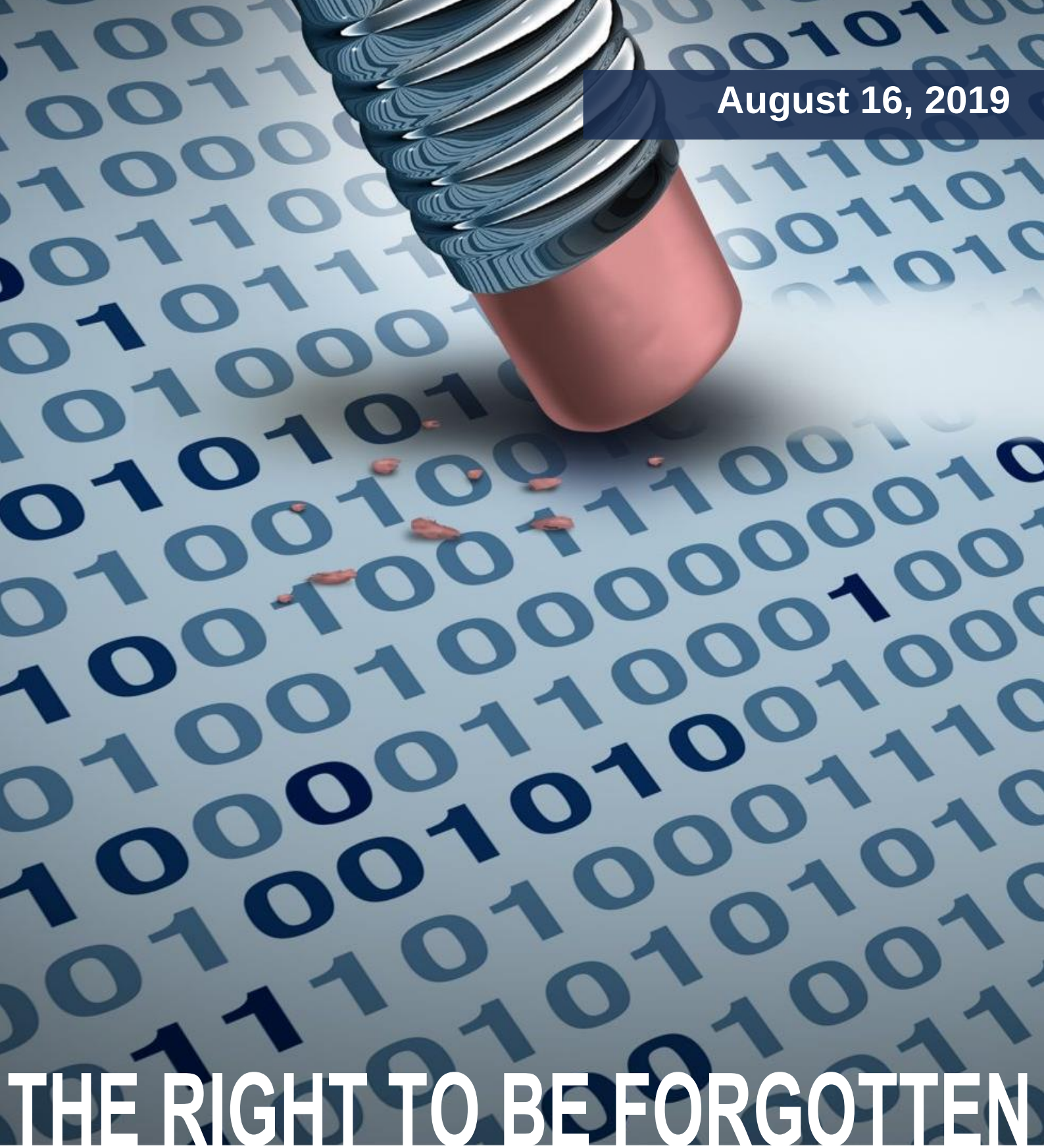

August 16, 2019

THE RIGHT TO BE FORGOTTEN

- UNDER THE PERSONAL DATA PROTECTION BILL 2018

argus partners
SOLICITORS AND ADVOCATES

MUMBAI I DELHI I BENGALURU I KOLKATA

Introduction

The Personal Data Protection Bill, 2018 ("**New DP Act**") has introduced in India the concept of an individual's "right to be forgotten". This right is currently not available under India's current data privacy regime which comes in the form of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**DP Rules 2011**") framed under the Information Technology Act, 2000 ("**IT Act 2000**").

The right to restrict or prevent continuing disclosure of personal data:

Section 27 of the New DP Act, which falls under chapter VI (*Data Principal Rights*) of the New DP Act, carves out the "right to be forgotten" in no uncertain terms. As per this section, every data principal shall have the right to restrict or prevent continuing disclosure of personal data (relating to such data principal) by any data fiduciary if such disclosure meets 1 (one) of the following 3 (three) conditions, namely the disclosure of personal data: (i) has served the purpose for which it was made or is no longer necessary; or (ii) was made on the basis of the data principal's consent and such consent has since been withdrawn; or (iii) was made contrary to the provisions of the New DP Act or any other law in force.

To avail of the aforementioned right to restrict or prevent continuing disclosure of personal data, an application has to be made, in such form and manner as may be prescribed, to an Adjudicating Officer[i], and such Adjudicating Officer should have reached the conclusion that any 1 (one) of the 3 (three) grounds mentioned above applies and also that 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.

In determining whether 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 or not, the Adjudicating Officer is required to have regard to factors such as: (a) the sensitivity of the personal data; (b) the scale of disclosure and the degree of accessibility sought to be restricted or prevented; (c) the role of the data principal in public life; (d) the relevance of the personal data to the public; and (e) 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.

Where any person finds that personal data, the disclosure of which has been restricted or prevented by an order of the Adjudicating Officer, does not satisfy the conditions required for the restriction or prevention of disclosure any longer, such person may apply for the review of that order to the Adjudicating Officer in the prescribed manner, following which the Adjudicating Officer shall review his/her order on the basis of the 5 (five) factors mentioned above.

Why isn't the data principal required to approach the data fiduciary first?

Interestingly, section 27 of the New DP Act does not require the data principal to make a request to the relevant data fiduciary to restrict or prevent continuing disclosure of personal data before approaching the Adjudicating Officer for enforcement of rights under the aforesaid section 27.

Even more interesting is that, section 28 of the New DP Act which details the conditions and procedures for the exercise of rights under chapter VI of the New DP Act, specifically disapplies the aforementioned section 27 of the New DP Act from meeting the procedural requirements of section 28 of the New DP Act. As per section 28 of the New DP Act, the exercise of any right under

chapter VI of the New DP Act (other than the rights under section 27 of the New DP Act) shall only be on the basis of a request made in writing to the data fiduciary with reasonable information to satisfy the data fiduciary of the identity of the data principal making the request and the data fiduciary shall acknowledge receipt of such request within such period of time as may be specified.

Why did the legislature feel that any petition to enforce the right to be forgotten ought to be taken to the Adjudicating Officer directly without giving the data fiduciary a chance to do the needful on its own initiative? Was the legislature worried that data fiduciaries may agree to "forget" personal data without putting up a fight, even if such forgetfulness is not called for, under the prescribed tests, in order to save themselves money and effort? Maybe the legislature felt that if it entrusted to Adjudicating Officers the duty of deciding if the tests laid out under section 27 of the New DP Act have been met, there would be less data removed from the public domain on account of the right to forget under section 27 of the New DP Act.

Genesis of the right to be forgotten

The right to be forgotten has its roots in a decision handed out by the European Court of Justice, in 2014, in the case of *Google Spain SL, Google Inc.* v. *Agencia Española de Protección de Datos, Mario Costeja González,*[ii]. In this case, a newspaper had published an article in 1998 relating to a forced property sale that was required to be made by one Mr. Mario Costeja Gonzalez in order to settle a social security debt. In 2009, Mr. Mario Costeja Gonzalez contacted the newspaper and requested that details of the forced property sale be removed from the public domain because searching for his name brought up the old article. When the newspaper denied the request stating that the same was a government ordered publication, Mr. Mario Costeja Gonzalez requested Google Spain SL ("**Google**") to remove the search result. Eventually, the courts in the European Union ruled that Google would be required to remove the search results, but that the newspaper would not have to remove the original article. The ruling effectively established precedence and validated the right to be forgotten as law, with various caveats. The European Court of Justice therefore held that the European citizens have a right to request that commercial search firms like Google, that gather personal information for profit, remove links to private information when asked, provided that such information is no longer relevant. The European Court of Justice found that the fundamental right to privacy is greater than the economic interest of a commercial firm and, in some cases, greater than the public interest in access to information.

Comparison with GDPR

The European Union's General Data Protection Regulation ("**GDPR**") also provides for the right to be forgotten, but this right, enshrined in article 17 of the GDPR, has a wider scope than that of section 27 of the New DP Act. Under the GDPR, data subjects[iii] can require the controller[iv] to erase all personal data concerning him or her held by such controller without undue delay. As mentioned above, under the New DP Act, data principals can only restrict or prevent continuing disclosure of personal data. They cannot require the data fiduciary to erase the personal data altogether. To avail of such a right of erasure under the GDPR, the data subject must be able to show that: (i) the purposes for which the personal data was collected or otherwise processed no longer exists; or (ii) the data subject has withdrawn consent on the basis of which the processing had commenced, and there is no other legal ground for the processing; or (iii) that the data subject is entitled to object to the processing of his personal data; or (iv) that the data subject's personal data has been unlawfully processed; or (v) the personal data is required to be erased for compliance with a legal obligation to which the controller is subject; or (vi) the personal data has been collected in relation to the offer of information society services directly to a child.

However, even under the GDPR, the right to be forgotten is not available to the extent that the processing of personal data is necessary: (a) for exercising the right of freedom of expression and information; (b) for compliance with a legal obligation or the performance of a task carried out in public interest; (c) for reasons of public interest in the area of public health; (d) for archiving

purposes in public interest, scientific or historical research purposes or statistical purposes if the exercise of the right to be forgotten is likely to restrict or obstruct the objectives of such archiving; or (e) for the establishment, exercise or defence of legal claims.

Unlike under the New DP Act, the GDPR envisages the data subject approaching the controller for erasure of personal data. Only if the data controller refuses to comply with such request can the data subject approach a supervisory authority for redressal. Article 58(2) of the GDPR provides that a supervisory authority shall have, *inter alia*, the corrective power to order the rectification or erasure of personal data or restriction of processing pursuant to article 17 of the GDPR.

Does the data storage limitation supplement the right to be forgotten?

Section 10 of the New DP Act states that a data fiduciary shall retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is processed. Further, it imposes an obligation on every data fiduciary to undertake periodic reviews in order to determine whether it is necessary to retain the personal data in its possession. If it is not necessary for personal data to be retained by a data fiduciary, then such personal data must be deleted in a manner as may be specified.

Thus, even if the right to be forgotten under section 27 of the New DP Act does not provide a right of erasure, the data storage limitation under section 10 of the New DP Act requires data fiduciaries to erase personal data on their own under certain circumstances.

The aforementioned section 10 of the New DP Act falls under chapter II of the New DP Act (*Data Protection Obligations*). Section 69(2) of the New DP Act, *inter alia*, states that, in the event a data fiduciary processes personal data or sensitive personal data or personal data of children in breach of chapter II of the New DP Act, the data fiduciary shall be liable to pay a fine of up to Rs. 15,00,00,000 (Rupees fifteen crore) or 4% (four percent) of its total worldwide turnover for the preceding financial year, whichever is higher.

However, the New DP Act does not provide data principals with an express right to compel data fiduciaries to cease to retain personal data when it is not required to retain such data. Chapter II of the New DP Act has been framed as a set of obligations on data fiduciaries and not as rights available to data principals (which are covered under chapter VI of the New DP Act). In contrast, chapter VI of the New DP Act (which includes the aforementioned “right to be forgotten” under section 27) is framed as a set of rights available to data principals. Further, there is no express provision for data principals to complain to the Data Protection Authority of India[v] to take action against a data fiduciary who holds on to personal data even after the need to retain it has passed.

It may be noted that section 97(6)(d) of the New DP Act states that the Data Protection Authority shall, no later than 12 (twelve) months from the notified date, issue codes of practice on storage limitation under section 10 of the New DP Act. The central government is required to notify a date within 12 (twelve) months of the enactment of the New DP Act. Various provisions of the New DP Act, including section 27 and section 10 shall come into force 18 (eighteen) months from the notified date. It is hoped that the codes of practice on storage limitation under section 10 of the New DP Act that are issued by the government provide for detailed procedures for the enforcement of the data storage limitation prescribed by the aforementioned section 10 of the New DP Act.

Impact of the right to be forgotten

Internet searches

Once the New DP Act comes into effect, an individual whose personal data appears on internet searches will be able to apply to an Adjudicating Officer for an order calling on 1 (one) or more

search engines to remove such personal data from the public domain provided the conditions stipulated under section 27 of the New DP Act are complied with, i.e., it can be shown that continuing disclosure of such personal data is no longer necessary or has served the purpose for which it was made. Further, the balance of interest between such removal and the right to freedom of speech and expression and the right to information of any other citizen, must be weighed in favour of such individual whose personal data is being removed. However, as discussed earlier, such individual will not be entitled to seek erasure of such personal data and such personal data may remain etched on servers and other storage spaces.

Personal data held in myriad other ways can also be restricted from further disclosure under the aforementioned section 27 of the New DP Act. Thus, the right to forget can be used to compel an employer to not disclose information pertaining to an ex-employee if it can be shown that such information, say a past act of indiscipline, is no longer relevant or pertinent.

Restricting disclosure of data held by a public authority

The right to be forgotten under section 27 of the New DP Act will be effective even if the data fiduciary who holds or processes the personal data is a public authority. In this context, a public authority could be a university or a government owned bank or hospital. When evaluating the balance of interest between such removal and the right to freedom of speech and expression and the right to information of other citizens, would the fact that the data fiduciary is a public authority weigh against the data principal? In our opinion, the nature or character of the data fiduciary should not make a difference, especially since elements such as the right to freedom of speech and expression and the right to information of other citizens have already been woven into section 27 of the New DP Act.

Journalistic exemption

Section 47 of the New DP Act exempts the processing of personal data which is necessary for, or relevant to, a journalistic purpose from various provisions of the New DP Act, including, *inter alia*, section 10 and section 27. Therefore, the right to be forgotten and the rule of data storage limitation will not apply if the personal data is held by a media organisation which is able to show that the processing of personal data is required for a journalistic purpose. "*Journalistic purpose*" is defined to mean any activity intended towards the dissemination through print, electronic or any other media of factual reports, analysis, opinions, views or documentaries regarding (i) news, recent or current events; or (ii) any other information which the data fiduciary believes the public, or any significantly discernible class of the public, to have an interest in. In other words, either the personal data should relate to current news or it should be a matter of public interest for this exemption to apply. Further, such processing for a journalistic purpose should also comply with any code of ethics issued by the Press Council of India or any media self-regulatory organisation.

The GDPR does not have an exception on the lines of section 47 of the New DP Act. However, article 85 of the GDPR (Processing and freedom of expression and information) requires Member States to reconcile the right to the protection of personal data with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression. For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States are required to provide for exemptions or derogations from chapter II (principles), chapter III (rights of the data subject), chapter IV (controller and processor), chapter V (transfer of personal data to third countries or international organisations), chapter VI (independent supervisory authorities), chapter VII (cooperation and consistency) and chapter IX (specific data processing situations) of the GDPR, if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.

Conflict between right to privacy in respect of personal data and the right to information:

As may be expected, there is bound to be a conflict between the right to privacy in respect of personal data and the right to information as enshrined under the Right to Information Act, 2005 ("**RTI Act**"). The RTI Act sets out a practical regime for Indian citizens to secure access to information under the control of public authorities. The RTI Act assumes that democracy requires an informed citizenry and transparency of information which are vital to its functioning and also to contain corruption and to hold governments and their instrumentalities accountable to the governed. It also assumes that the revelation of information in actual practice is likely to conflict with other public interests including efficient operations of the governments, optimum use of limited fiscal resources and the preservation of confidentiality of sensitive information. The RTI Act seeks to harmonise these conflicting interests while preserving the paramountcy of the democratic ideal.

Section 8 of the RTI Act contains a number of exemptions from the disclosure of information relating to, or under the control of, public authorities, by a public information officer. There is no obligation to give information to any citizen if disclosure of such information would prejudicially affect the sovereignty and integrity of India or if there is a court order forbidding the disclosure of such information or disclosure would cause a breach of privilege of Parliament or the State Legislature or if the information involves trade secrets or intellectual property and its disclosure would harm the competitive position of a third party, unless larger public interest warrants such disclosure, and the like. Sub-section (j) of section 8 of the RTI Act provides an exemption from public disclosure for personal data, though it does not use the term 'personal data'. As per section 8(1)(j) of the RTI Act, there shall be no obligation to give any citizen information which relates to 'personal information' (sic) if the disclosure of such personal information has no relationship to any public activity or interest, or if it would cause unwarranted invasion of the privacy of the relevant individual, unless officials created and empowered under the RTI Act such as the Central Public Information Officer or the State Public Information Officer or the appellate authority, as the case may be, are satisfied that the larger public interest justifies the disclosure of such information.

Overlap between section 8(1)(j) of the RTI Act and the right to be forgotten under the New DP Act:

The main difference between the exemption (against disclosure) under section 8(1)(j) of the RTI Act and the right to be forgotten under section 27 of the New DP Act, is that, in the latter, the data principal can proactively take steps to restrict or prevent the continuing disclosure of his or her personal data by petitioning an Adjudicating Officer. In the former, a public official (such as the Central Public Information Officer or the State Public Information Officer or the appellate authority), from whom any information has been demanded, can refuse to provide such information on the basis of the exemption given in section 8(1)(j) of the RTI Act. Section 11 of the RTI Act read with section 7(7) of the RTI Act requires Central Public Information Officers and State Public information Officers, before disclosing any information relating to a third party pursuant to a request under section 6 of the RTI Act, to give a written notice and seek a submission (in writing or orally) from such third party who has either supplied such information or has requested for it to be kept confidential. Such submission of the third party has to be taken into account while taking a decision about disclosure of information. Other than the right to make a submission when called upon to do so, the third party has little or no say in the disclosure of information.

Proposed amendment of section 8(1)(j) of the RTI Act by the New DP Act:

The New DP Act proposes to amend the aforementioned sub-section (j) of section 8 of the RTI Act. The amendatory language is provided in the second schedule to the New DP Act and it uses

terms which tie in with the terminology of the New DP Act. The proposed amendment provides that personal data need not be disclosed under the RTI Act if such disclosure if likely to cause 'harm' to a data principal, where such 'harm' outweighs the public interest in accessing such information having due regard to the common good of promoting transparency and accountability in the functioning of the public authority. The proposed amendment to the RTI Act also states that terms such as 'personal data', 'data principal', and 'harm' shall have the meaning assigned to such terms in the New DP Act.

The scope of the term 'harm' under the New DP Act is fairly wide and includes, *inter alia*, loss of reputation or humiliation, restriction placed or suffered directly or indirectly on any action arising out of a fear of being observed or placed under surveillance. Further, the amended exemption will apply if there exists the mere likelihood that the disclosure of personal data will cause 'harm' to a data principal. Under the existing exemption, a mere likelihood of harm is not sufficient. The disclosure should actually cause an unwarranted invasion of the privacy of the relevant individual.

Thus the proposed amendment to the RTI Act substantially widens the scope of the current exemption under section 8(1)(j) of the RTI Act and gives more leeway to information officers for rejecting a request for disclosure of information. If implemented, this amendment will curb citizens' right to information.

This note has been written by Vinod Joseph (Partner) and Deeya Ray (Associate).

DISCLAIMER

This document is merely intended as an update and is merely for informational purposes. This document should not be construed as a legal opinion. No person should rely on the contents of this document without first obtaining advice from a qualified professional person. This document is contributed on the understanding that the Firm, its employees and consultants are not responsible for the results of any actions taken on the basis of information in this document, or for any error in or omission from this document. Further, the Firm, its employees and consultants, expressly disclaim all and any liability and responsibility to any person who reads this document in respect of anything, and of the consequences of anything, done or omitted to be done by such person in reliance, whether wholly or partially, upon the whole or any part of the content of this document. Without limiting the generality of the above, no author, consultant or the Firm shall have any responsibility for any act or omission of any other author, consultant or the Firm. This document does not and is not intended to constitute solicitation, invitation, advertisement or inducement of any sort whatsoever from us or any of our members to solicit any work, in any manner, whether directly or indirectly.

You can send us your comments at:
argusknowledgecentre@argus-p.com

Mumbai I Delhi I Bengaluru I Kolkata

www.argus-p.com

[i] Appointed under section 68 of the New DP Act
[ii] *Google Spain SL, Google Inc.* v. *Agencia Española de Protección de Datos, Mario Costeja González*,ILEC 060 (CJEU 2014)
[iii] The GDPR uses the term "data subject" instead of "data principal"
[iv] The GDPR uses the term "controller" instead of "data fiduciary"
[v] Appointed under section 49 of the New DP Act