April 17, 2020

MALICIOUS PERSONAL DATA BREACH BY AN EMPLOYEE

- CONSEQUENCES

argus partners
SOLICITORS AND ADVOCATES

TECHNOLOGY & DATA PRIVACY

MUMBAI I DELHI I BENGALURU I KOLKATA I AHMEDABAD

1. Introduction

1.1. Let's consider the following hypothetical situation. The employee ("Employee") of a reputed hospital in India, working in the hospital's maintenance department, had a quarrel with his immediate supervisor regarding his pay hike, which the Employee felt was meagre. Feeling very aggrieved, the Employee intentionally and maliciously, disclosed on his Facebook page, the names of a few celebrities who had undergone treatment at that hospital in the last five years, for lifestyle related illnesses such as heart disease, diabetes, blood pressure, etc. Details of the treatment undergone and length of the hospital stay were also disclosed, along with a proclamation that the hospital was 'useless'. The hospital had put in place reasonable security practices as per the IS/ISO/IEC 27001 standard to safeguard the privacy of its patients' personal data, but those safeguards were circumvented by the Employee, who was promptly dismissed from service by the hospital. The celebrities whose details were wantonly leaked want to be compensated for the trauma and mental agony that they have undergone as well as the loss of reputation. Since the Employee does not have deep pockets, the celebrities are planning to pin liability on and claim compensation from the hospital for the actions of its employee. Over and above claiming compensation from the hospital, the celebrities would also like to see the Employee suffer the consequences of his actions.

1.2. In this paper, we examine if it would be possible for the celebrities to claim compensation from the hospital either under a statute or through a claim for vicarious liability under tort law. We also analyse the possible consequences for the Employee as a result of his personal data breach. For this purpose, we review (i) the existing Indian data privacy regulation, namely the Information Technology Act, 2000 ("IT Act") and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("2011 DP Rules") (ii) the Personal Data Protection Bill, 2019 ("PDP Bill 2019"), (iii) Indian tort law and (iv) English common law relating to an employer's vicarious liability for his/her employee's tort.

2. Liability under existing Indian statutes and rules

2.1. *Nature of the disclosed information*

Rule 3 of the 2011 DP Rules lists eight types of sensitive personal data, two of which are "physical, physiological and mental health condition" and "medical records and history". Thus, it is clear that the information disclosed by the Employee is sensitive personal data.

2.2. *Section 43A of the IT Act*

2.2.1. For the employer:

Section 43A of the IT Act provides that where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Explanation (ii) to the aforementioned section 43A states that "*reasonable security practices and procedures*" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or

impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

Rule 8 of the 2011 DP Rules provides that a person shall be considered to have complied with reasonable security practices and procedures, if it has implemented such security practices and standards and has a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business. Rule 8(2) provides that the International Standard IS/ISO/IEC 27001 on "Information Technology – Security Techniques - Information Security Management System - Requirements" meets the standards referred to above. A person may follow standards other than IS/ISO/IEC codes of best practices for data protection, provided such codes of best practices are (i) duly approved and notified by the Central Government and (ii) certified or audited on a regular basis by an independent auditor, who is duly approved by the Central Government. The audit of reasonable security practices and procedures shall be carried out by an auditor at least once a year or as and when the body corporate undertakes significant upgradation of its process and computer resource.

A person who has implemented either the IS/ISO/IEC 27001 standard or any codes of best practices for data protection which are approved and notified by the Central Government, shall be deemed to have complied with reasonable security practices and procedures.

The hospital does not have in place any agreement with its patients, which spells out the security practices and procedures the hospital ought to have, to secure the privacy of its patients' data. However, since the hospital has implemented IS/ISO/IEC 27001 standard security control measures, it will be entitled to the safe harbour created by the 2011 DP Rules and will not be liable to pay compensation to the celebrities under the aforesaid section 43A.

2.2.2. For the Employee:

Section 43A of the IT Act would apply to the Employee only if the Employee is a body corporate. A body corporate is defined as follows:

> "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities."

The Employee is involved in a professional activity, but since he is an individual, he would fall within this definition only if he is a sole proprietorship, which he is not. Therefore, section 43A of the IT Act would not apply to the Employee and it would not be possible for the celebrities to claim compensation from the Employee under section 43A of the IT Act.

2.3. *Section 72A of the IT Act*

2.3.1. For the employer:

Section 72A of the IT Act penalises any person who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain, discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person. Any person found guilty under the aforesaid section 72A shall be punished with imprisonment for a

term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.

The information disclosed by the Employee on his Facebook page was obtained by the hospital under the terms of a lawful contract, namely a contract to provide medical services. However, the disclosure was not by the hospital, but by the Employee. Even though the Employee's action was intentional, it would not be possible to impute the same to the hospital, especially for the imposition of a criminal penalty under the aforesaid section 72A.

2.3.2. For the Employee:

Section 72A of the IT Act will apply to the Employee, since all of its ingredients have been met.

A lawful contract was in place between the hospital and each of the celebrities. The sensitive personal data processed by the hospital was secured through such contract. The Employee made the wrongful disclosure intentionally, in order to cause wrongful loss to the celebrities. The Employee would argue that section 72A requires the person accused under section 72A to have secured access to the sensitive personal data while providing services under the terms of a lawful contract. The Employee did not have a contract with the celebrities at all and he wasn't providing them any service directly. This argument is unlikely to be sustained. Even if section 72A is interpreted on the lines of the Employee's argument, it can be said that there was a lawful (employment) contract between the hospital and the Employee, the Employee was rendering services to the hospital under such contract and the Employee secured access to the celebrities' sensitive personal data while providing services to the hospital under the terms of his employment contract.

2.4. *The 2011 DP Rules*

2.4.1. For the employer:

The 2011 DP Rules impose a number of obligations on the employer, which can be summarised as follows:

- The hospital is required to have a privacy policy, which must be available for viewing by those who have provided any information to the hospital under a lawful contract. The privacy policy must be published on the hospital's website. The privacy policy has to clearly set out the practices and policies of the hospital for the collection, receipt, possession, storage, dealing or handling of information. It should also list out the types of personal data or sensitive personal data collected by the hospital.
- When collecting sensitive personal data from any patient, the patient's prior consent ought to have been obtained. Further, sensitive personal data may be collected only for a lawful and necessary purpose. The sensitive personal data should not be retained for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force.
- The provider of sensitive information should be given the option to withdraw the consent given to the hospital earlier. Patients have the right to review the information that they have provided and ensure that any personal data found to be inaccurate or deficient is corrected or amended to the extent it is feasible.

The 2011 DP Rules do not contain any penal provision and if the hospital is in breach of any of the obligations mentioned above, it will be liable under the residuary penal provision contained in section 45 of the IT Act, which is discussed below in paragraph 2.5.

2.4.2. For the Employee:

The obligations cast by the 2011 DP Rules fall on a body corporate. In some cases, such obligations also fall on 'a person acting on behalf of a body corporate'. As mentioned above, the Employee is not a 'body corporate', but may be termed as 'a person acting on behalf of a body corporate'.

Rule 6(1) of the 2011 DP Rules provide that the disclosure of sensitive personal data or information by a body corporate to any third party shall require prior permission from the provider of such information, who has provided such information under lawful contract or otherwise, unless such disclosure has been agreed to in the contract between the body corporate and provider of information, or where the disclosure is necessary for compliance of a legal obligation. The aforesaid Rule 6(1) applies only to body corporates and not to 'a person acting on behalf of a body corporate'. Therefore, this Rule shall not apply to the Employee.

Rule 6(3) of the 2011 DP Rules blandly states that 'the body corporate or any person on its behalf shall not publish the sensitive personal data or information' (sic). There is no reference to 'consent' in this sub-rule and it is not easy to distinguish it from the obligation under Rule 6(1) to not disclose sensitive personal data without the consent of the data principal. However, on a plain reading of this sub-rule, the Employee is in breach of this sub-rule.

As mentioned earlier, the 2011 DP Rules do not contain any penal provision for any breach of the 2011 DP Rules and the Employee will be liable for breach of Rule 6(3) of the 2011 DP Rules under the residuary penal provision contained in section 45 of the IT Act, which is discussed below in paragraph 2.5.

2.5. *Section 45 of the IT Act*

Section 45 of the IT Act is a residuary clause which provides that whoever contravenes any rules or regulations made under the IT Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding Rs. 25,000 (Rupees twenty five thousand) to the person affected by such contravention or a penalty not exceeding Rs. 25,000 (Rupees twenty five thousand).

2.5.1. For the employer:

Since the hospital has not been in breach of any provision of the IT Act or the 2011 DP Rules, it would not be possible to claim compensation from the hospital under section 45.

2.5.2. For the Employee:

Since the Employee has been in breach of Rule 6(3) of the 2011 DP Rules for which no specific penalty has been provided, he would be liable to pay compensation of an amount not exceeding Rs. 25,000 to each of the celebrities under section 45.

3. Liability under the PDP Bill 2019

3.1. *Nature of the disclosed information*

Section 3(36) of the PDP Bill 2019 has an exhaustive list of various types of sensitive personal data and one of the listed categories of sensitive personal data is 'health data'. Section 3(21) of the PDP Bill 2019 says that "health data" means the data related to the state of physical or mental health of the data principal and includes records regarding the past, present or future state of the health of such data principal, data collected in the course of registration for, or provision of health services, data associating the data principal to the provision of specific health services. Therefore, it is clear that the information disclosed on Facebook by the Employee is sensitive personal data.

3.2. *Section 64 of the PDP Bill 2019*

3.2.1. Section 64(1) of the PDP Bill 2019 provides that any data principal who has suffered harm as a result of any violation of any provision under the PDP Bill 2019 or the rules or regulations made thereunder, by a data fiduciary or a data processor, shall have the right to seek compensation from the data fiduciary or the data processor, as the case may be. The explanation to this section 64(1) clarifies that a data processor shall be liable to a data principal only where it has acted outside or contrary to the instructions of the data fiduciary pursuant to section 31[1], or where the data processor is found to have acted in a negligent manner, or where the data processor has not incorporated adequate security safeguards under section 24[2], or where it has violated any provisions of the PDP Bill 2019 expressly applicable to it.

3.2.2. Therefore, if a data processor acts as per the instructions of its data fiduciary, even if its actions result in a personal data breach and cause loss or damage to a data principal, the data principal will not be able to make a claim against such data processor. Presumably, in such a situation, the data fiduciary would be in breach of the PDP Bill 2019 (on account of giving instructions which result in a personal data breach) and it would be possible for the data principal to make a claim against the data fiduciary in respect of the loss or damage suffered by the data principal.

3.2.3. For the employer:

The facts mentioned above suggest that the hospital has put in place reasonable security practices and procedures and been in compliance with the law. Even if the hospital has committed any procedural breach of applicable data privacy laws, the damage suffered by the celebrities did not arise out of such breach. The damage was solely on account of an intentional action of the Employee, which was not in the course of his employment. For a discussion on what would or would not constitute an action in the course of employment, please refer to paragraph 5.3 below (*Indian case law*).

Therefore, it would not be possible for the celebrities to claim compensation from the hospital under section 64 of the PDP Bill 2019.

[1] Section 31 mandates the existence of a contract between the data fiduciary and the data processor for the data processor to process personal data. Such data processors appointed or engaged by a data fiduciary cannot involve any other data processor in processing on its behalf, except without the permission of the data fiduciary and unless permitted in the contract. Processing of data by (i) data processor or (ii) any employee of the data processor or the data fiduciary, shall only be as the data fiduciary instructs and shall be treated as confidential.

[2] Section 24 mandates every data processor and data fiduciary to implement security safeguards, having regard to the nature, scope and purpose of processing personal data, the risks associated with such processing, and the likelihood and severity of the harm that may result from such processing. Such security safeguards have to be reviewed periodically. The safeguards shall include: (a) use of methods such as de-identification and encryption; (b) steps necessary to protect the integrity of personal data; and (iii) steps necessary to prevent misuse, unauthorised access to, modification, disclosure or destruction of personal data.

3.2.4. For the Employee:

The Employee would be liable under section 64 only if the Employee is either a data fiduciary or a data processor. The PDP Bill 2019 says that a "data fiduciary" means any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data. Since the Employee does not determine the purpose and means of processing of personal data received by the hospital, the Employee would not be a data fiduciary. The PDP Bill 2019 says that a "data processor" means any person, including the State, a company, any juristic entity or any individual, who processes personal data on behalf of a data fiduciary. It could be argued that the Employee is a data processor. However, such an interpretation would be contrary to the business understanding of who a data processor is, which is that, a data processor is an entity that is distinct from the data fiduciary, but processes data received from the data fiduciary, on the instructions of the data fiduciary, for a fee. Further, section 31(3) of the PDP Bill 2019 says that the data processor, and any employee of the data fiduciary or the data processor, shall only process personal data in accordance with the instructions of the data fiduciary and treat it confidential. This implies that employees of the data fiduciary or of the data processor are distinct from the data processor itself. In the European Union's first data privacy directive[3], the definition of a data processor specifically excluded employees of the data processor. The GDPR[4] is silent on this point though.

Since the Employee is neither a data fiduciary nor a data processor, he will not be liable under section 64 of the PDP Bill 2019.

3.3. *Criminal liability under the PDP Bill 2019*

The PDP Bill 2019 does not penalise a person who knowingly or intentionally or recklessly discloses any data principal's personal data causing harm to such data principal. Section 90 of the previous version of the PDP Bill 2019, namely the Personal Data Protection Bill, 2018 ("PDP Bill 2018") had provided that any person who knowingly, intentionally or recklessly obtains or discloses or transfers or sells '*personal data*' to another person in contravention of the PDP Bill 2018, and it results in '*significant harm*' to a data principal, then such person shall be punishable with imprisonment for a term not exceeding 3 (three) years and/or shall be liable to a fine which may extend up to Rs. 2,00,000 (Rupees two lac). If the data happens to be '*sensitive personal data*', then section 91 of the PDP Bill 2018 upped the ante such that, if mere '*harm*' is caused to a data principal, the punishment could be imprisonment for a term not exceeding 5 (five) years and/or a fine which may extend up to Rs. 3,00,000 (Rupees three lac).

The aforementioned penal provisions have been left out from the PDP Bill 2019, possibly since they overlap with Section 72A of the IT Act 2000. The main difference between section 72A of the IT Act and sections 90 and 91 of the PDP Bill 2018 is that in the former, the offender has to be a person who legitimately secured access to personal information before making a wrongful disclosure. Under the PDP Bill 2018, any person who made a wrongful disclosure of personal data, howsoever such personal data may have come into the possession of the discloser, could be liable.

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

3.4. *Section 61 of the PDP Bill 2019*

3.4.1. The PDP Bill 2019 has a residuary penalty clause in section 61 which states that where any person fails to comply with any provision of the PDP Bill 2019, or rules prescribed or regulations specified thereunder as applicable to such person, for which no separate penalty has been provided, such person shall be liable to a penalty subject to a maximum of Rs. 1,00,00,000 (Rupees one crore) in case of significant data fiduciaries, and a maximum of Rs. 25,00,000 (Rupees twenty five lac) in all other cases.

3.4.2. For the employer:

For a claim to be made against the hospital under the aforesaid section 61, the hospital ought to have failed to comply with any provision of the PDP Bill 2019, for which a specific penalty hasn't been provided. As mentioned earlier, the hospital has complied with all its statutory obligations and therefore, a claim would not lie against the hospital under the aforesaid section 61.

Would it be possible to make a claim on the hospital under section 61 for a breach by the Employee of a provision for which a specific penalty hasn't been provided? The answer would be no, for the following reason. Unlike the residuary clause in 2011 DP Rules which requires a violator to pay compensation to the person affected by such contravention not exceeding Rs. 25,000 (Rupees twenty five thousand) or a penalty not exceeding Rs. 25,000 (Rupees twenty five thousand), the residuary clause in the PDP Bill 2019 only provides for a penalty. Vicarious liability is a civil law concept and would not apply in the case of a penalty.

3.4.3. For the Employee:

The Employee has been in breach of sections 4 and 5 of the PDP Bill 2019.

Section 4 of the PDP Bill 2019 provides that no personal data shall be processed by any person, except for any specific, clear and lawful purpose. The disclosure of the celebrities' sensitive personal data by the Employee was not for a lawful purpose and would result a breach of the aforesaid section 4.

Section 5 of the PDP Bill 2019 provides that every person processing personal data of a data principal shall process such personal data in a fair and reasonable manner and ensure the privacy of the data principal. The processing of the personal data should also be for a purpose consented to by the data principal or which is incidental to or connected with such purpose, and which the data principal would reasonably expect that such personal data shall be used for, having regard to the purpose, and in the context and circumstances in which the personal data was collected. The Employee is in breach of the aforesaid section 5 as well.

Both the aforesaid sections 4 and 5 fall under Chapter II of the PDP Bill 2019, which deals with obligations of a data fiduciary. However, the language of the aforesaid sections 4 and 5 is such that they apply to any individual processing personal data. Since the PDP Bill 2019 does not prescribe any separate penalty for a breach of either section 4 or 5, the Employee shall be liable to a penalty not exceeding Rs. 25,00,000 (Rupees twenty five lac) for each of section 4 and section 5. It should be noted that any penalty levied on the Employee under section 61 of the PDP Bill 2019, will be credited to the Consolidated Fund of India and shall not be paid to any of the celebrities as compensation.

4. Follow-on obligations under the PDP Bill 2019

4.1. *Hospital's obligation to report the breach*

Section 25 of the PDP Bill 2019 requires every data fiduciary to inform the Data Protection Authority of India ("Authority") by notice about the breach of any personal data processed by the data fiduciary where such breach is likely to cause harm to any data principal. It is irrelevant whether the breach took place due to a fault on the part of the data fiduciary or not.

A "personal data breach" has been defined by the PDP Bill 2019 to mean any unauthorised or accidental disclosure of, acquisition of, sharing of, use of, alteration of, destruction of, loss of access to, personal data that compromises the confidentiality, integrity or availability of personal data to a data principal.

Section 25(3) of the PDP Bill 2019 provides that the notice under section 25 of the PDP Bill 2019 shall be made by the data fiduciary to the Authority as soon as possible and within such period, as may be specified by the regulations made by the Authority under the PDP Bill 2019 following the breach after accounting for any period that may be required to adopt any urgent measures to remedy the breach or mitigate any immediate harm. Further, section 25(4) of the PDP Bill 2019 provides that where it is not possible to provide all the required information, at the same time, the data fiduciary shall provide such information to the Authority in phases without undue delay.

The notice sent by the data fiduciary is required to include particulars such as (a) the nature of personal data which is the subject matter of the breach, (b) the number of data principals affected by the breach, (c) the possible consequences of the breach and (d) the action being taken by the data fiduciary to remedy the breach.

In light of the above, the hospital, being a data fiduciary, shall be required to report the unauthorised, malicious disclosure of the celebrities' personal data by its Employee to the Authority, in accordance with section 25 of the PDP Bill 2019.

The hospital is also under a duty to take all possible mitigatory steps after any personal data breach occurs. Therefore, the hospital should take all possible steps to compel the Employee to delete his Facebook posts. For this purpose, the hospital would be required to contact Facebook's administrators and file an official complaint.

It may be noted that as per section 57(1)(a) of PDP Bill 2019 in the event the data fiduciary contravenes its obligation to take prompt and appropriate action under section 25 of the PDP Bill 2019, in response to a data security breach, such data fiduciary shall be liable to a penalty which may extend to Rs. 5,00,00,000 (Rupees five crore) or 2% (two percent) of its total worldwide turnover of the preceding financial year, whichever is higher.

4.2. *Authority's duties after receiving a report under section 25*

Upon receipt of a notice under section 25 of the PDP Bill 2019, the Authority:

- shall determine whether such breach should be reported by the data fiduciary to the data principal, taking into account the severity of the harm that may be caused to such data principal[5];

[5] Section 25(5) of the PDP Bill 2019.

- may require the data fiduciary to conspicuously post details of the personal data breach on the data fiduciary's website[6];
- may post details of the data fiduciary's personal data breach on its own website[7]; and
- direct the data fiduciary to take appropriate remedial action as soon as possible[8].

As per section 49(2)(b) of the PDP Bill 2019, the Authority is required to take prompt and appropriate action in response to any personal data breach in accordance with the provisions of the PDP Bill 2019. As per section 51 of the PDP Bill 2019, the Authority may, for the discharge of its functions under the PDP Bill 2019, issue such directions from time to time as it may consider necessary to any data fiduciary or data processor who shall be bound to comply with such directions.

5. The hospital's vicarious liability under tort law

5.1. The expression 'vicarious liability' signifies the liability which a person, A, may incur towards a third party, C, for the damage caused to C by the negligence of, or any other tort committed by, another person, B. A's liability towards C arises (i) on account of A's relationship with B, which could be that of an 'employer-employee', a 'master-servant' etc. and (ii) because B committed the tort against C in the course of his employment. It is not necessary for A to have participated in the commission of the tort in any way nor is it necessary for A to have breached any duty that A owed under law to C, as long as the tort was committed by his servant or employee in the course of employment. The doctrine of vicarious liability is based on the maxims *respondeat superior* (i.e. let the principal be liable) and *qui facit per alium facit per se* (i.e. he who does an act through another does it himself).[9]

5.2. *Do the IT Act, the 2011 DP Rules or the PDP Bill 2019 exclude a tort law claim against the hospital?*

Are the IT Act, 2011 DP Rules and the PDP Bill 2019 meant to be comprehensive and exhaustive, so as to bar any claim being made on the hospital, by the celebrities, outside the PDP Bill 2019? It is an accepted principle of law that once a statute has been enacted to regulate a particular type of activity or to prevent any mischief, any claim or lawsuit relating to such activity or mischief must be made under such statute. However, section 65 of the PDP Bill 2019 provides that no compensation awarded, or penalty imposed, under this Act shall prevent the award of compensation or imposition of any other penalty or punishment under this Act or any other law for the time being in force. That even if an action is penalised under a statute, a claim for compensation under tort law is not excluded, is also a well-accepted accepted principle of law.

The IT Act and the PDP Bill 2019 not only penalise personal data breaches, but also provide for the payment of compensation in certain specific cases of personal data breach. However, none of these statutes provide for vicarious liability to be fastened on an employer for loss or damage arising out of the personal data breach of an employee. Since the PDP Bill 2019 is silent on the aspect of an employer's vicarious liability for acts of the employee, the celebrities will not be precluded from making a tort law claim on the hospital, for the actions of the Employee, on the basis of the hospital's vicarious liability.

[6] Section 25(6) of the PDP Bill 2019.
[7] Section 25(7) of the PDP Bill 2019.
[8] Section 25(6) of the PDP Bill 2019.
[9] D. Kavitha and R. Dhivya, "*A Comparative Study on Vicarious Liability in Torts and Administrative Law in India*", International Journal of Pure and Applied Mathematics, (2018) Vol. 120, no. 5, 1849-1864. Available at: https://acadpubl.eu/hub/2018-120-5/2/171.pdf.

5.3. *Indian case law*

We do not have any Indian case law dealing with vicarious liability in the context of a personal data breach. However, the following cases dealing with vicarious liability are nevertheless relevant.

(a) *Sitaram Motilal Kalal* vs*. Santanuprasad Jaishankar Bhatt*[10]

The owner of a car entrusted it to A to ply it as a taxi. B used to clean the taxi and was either employed by the owner or by A. A trained B to drive the vehicle and took B for his driving licence test. While taking the test, B caused bodily injury to the respondent. At the time of the accident, A was not present inside the vehicle. On the question of whether the owner was liable for the accident, it was held by the Court that the owner was not liable because the evidence did not disclose that owner had employed B to drive the taxi or given him permission to drive the taxi. The Court found that A and B were not acting in the course of the owner's business. The Court held that there was no proof that A was authorized by the owner to coach B so that B might become a driver and drive the taxi. It appeared more probable that A wanted someone to assist him in driving the taxi for part of the time and was training the B to share the task of driving. According to the Court, at the time of the accident, the car was not being used as a taxi for the owner's business. The car was engaged in the work of B who had no connection with the owner's business. The owner's plea that it had not given any such authority was accepted by the Court. Holding that it had not been proved that the act was impliedly authorized by the owner or that it came within any of the extensions of the doctrine of scope of employment, the Court held that the owner was not vicariously liable. According to the Court, the test was whether the act was done on the owner's business or that it was proved to have been impliedly authorized by the owner. The Court opined that the law was settled that master is vicariously liable for the acts of his servants acting in the course of his employment. If a servant, at the time of an accident is not acting within the course of employment, but is doing something for himself, the master is not liable. Unless the act is done in the course of employment, the servant's act does not make the employer liable.

(b) *Pushpabai Purshottam Udeshi and Ors.* vs*. Ranjit Ginning and Pressing Co. (P) Ltd. and Ors*.[11]

One Purshottam Udeshi was travelling in a car owned by the respondent company, which was driven by its manager in a rash and negligent manner. The manager was travelling on the car owner's business and had permitted Purshottam to ride in the car. The car dashed against a tree resulting in the death of Purshottam. Purshottam's widow and children filed a claim for compensation against the manager as well as the respondent company. While discussing the principles of vicarious liability to ascertain whether the incident took place during the course of employment of the manager, the Court held that a master's liability was based on the ground that the impugned act was done in the scope or course of his employment or authority. Relying on the principles laid down in the case of *Sitaram Motilal Kalal vs. Santanuprasad Jaishankar Bhatt*, the Supreme Court stated that for the master's liability to arise, the act must be a wrongful act authorised by the master or a wrongful and unauthorised mode of doing some act authorised by the master. However, the Court pointed out that the recent trend in law was an extension of this doctrine of scope of employment to make the master liable for acts which did not strictly fall within the terms "in the course of the employment" as ordinarily understood. The Court, relied on the observations of Lord Denning in *Ormrod v. Crosville Motor Services Ltd* (which were agreed to by the Supreme Court in the case of *Sitaram Motilal Kalal vs. Santanuprasad Jaishankar Bhatt*) which stated that while it

[10] AIR1966SC1697.

[11] AIR1977SC1735.

was generally understood that the owner of a vehicle is only liable for the negligence of the driver if that driver is his servant acting in the course of his employment, this view was incorrect. The owner would also liable if the driver was, with the owner's consent, driving the car on the owner's business or for the owner's purposes. The Supreme Court stated this extension was accepted by the Court and consequently held the respondent-company vicariously liable in respect of the accident, holding the accident to have taken place during the course of employment.

(c) *State Bank of India* vs*. Shyama Devi*[12]

The plaintiff had a savings account with the State Bank of India. The plaintiff had handed over to an employee of the bank who was a friend of the plaintiff's husband and their neighbour, a cheque and cash to be credited to her account. She also sent the bank's employee a letter containing instructions and her pass-book. The employee misappropriated the amount and made false entries in the pass-book. The employee was not in charge of the savings bank counter at which the savings account of the plaintiff was dealt with and the cheque and cash were not handed over to the relevant person in charge. The question before the Court was whether the bank was liable to compensate the plaintiff. The Supreme Court held that the bank was not liable for the fraud committed by the employee as the employee did not have any authority to accept the cheque or cash to be deposited to the savings bank account on behalf of the State Bank of India. Moreover, the monies were not received by him in the normal course of business of the bank. According to the Court, the onus was on the plaintiff to show that she paid the amount to an employee of the bank and was received by that employee in the course of his employment, to make the bank liable. The false and fraudulent entry about the deposit of this amount in the pass-book, could not shift the onus on the bank to prove the contrary. The Court held that the employee's fraud was not in the course of employment and at the most, it could be said that him being an employee of the bank and a friend of the plaintiff's husband gave him an opportunity to commit the fraud.

(d) *State of Maharashtra and Ors.* vs*. Kanchanmala Vijaysing Shirke and Ors*[13].

A man riding a scooter was hit by a jeep which belonged to the State Government of Maharashtra. The person who was driving the jeep at the time of the accident was a clerk in Engineering Fishing Project Division, Ratnagiri, who was not the designated driver of the jeep. The scooter rider later succumbed to his injuries and his relatives sought compensation from the State on the grounds of vicarious liability. The Court explained the principles of vicarious liability, stating that a master would be liable even for acts which he has not authorised provided they are so connected with acts which he has been so authorised. However, if the act of the servant was not even remotely connected within the scope of employment and was an independent act, the master would not be responsible as the servant would not be acting in the course of his employment but would've gone outside.

The Court observed that the jeep was used for bringing employees to the office, and therefore was being used in connection with the affairs of the State and for an official purpose. The clerk was driving the vehicle under the authority of the "official driver" who was in charge of the said vehicle. The latter had permitted the clerk to drive the vehicle that night. According to the Court, an authorised act was being done in an unauthorised manner and that the accident took place when the act authorised was being performed in a mode which was not proper but nonetheless it was directly connected with 'in the course of employment'. The Court negated the contention that it was an independent act for a purpose or business which had no nexus or connection with the business of the State Government so as to absolve the State from the liability. The Court reasoned

[12] AIR1978SC1263.
[13] (1995)5SCC659.

that the crucial test was whether the initial act of the employee was expressly authorised and lawful. Since in the present case, the driver of the vehicle had been fully authorised to drive the jeep for a purpose connected with the affairs of the State and by allowing the clerk, who was also going on an official duty, to drive the jeep, when the accident took place, the negligent act of the driver and clerk was `in the course of employment', and consequently the State was made liable for the same.

(e) *Anita Bhandari and Ors.* vs*. Union of India (UOI) and Ors*.[14]

The petitioner's husband had gone to the respondent bank for a banking transaction and parked his scooter in front of the bank. At that time, the bank's cash box was being brought into the bank's premises. Therefore, the security guard objected to the petitioner's husband parking his scooter in front of the bank and subsequently he shot at the petitioner's husband who died on the spot.

While adjudging the liability of the respondent bank, the Gujarat High Court held that the act of the security guard could not be considered an independent act which would absolve the bank of vicarious liability. According to the High Court, since the unlawful act of the security guard was so connected with the authorized act of ensuring the cash box being safely brought into the bank, the unlawful act was a part of the mode of performing the authorized act and the fact that that if the employer were present on the spot it would not have authorized the security guard to fire at the deceased did not mean that the act was not done in the course of employment. The High Court reasoned that the moment the bank employed the security guard and entrusted him with a gun, it necessarily left it to him to determine and adjudge when the gun is to be used and trusted him for the manner in which it is done and consequently the bank was to be held answerable for the security guard's wrong not only in the wrong manner of using the gun but also in using the gun under the circumstance in which it ought not to have been done. The shooting of the deceased by the security guard could not be said to have been done from any caprice of the security guard. The High Court held that the act in question was in the course of employment of the security guard with the respondent bank and the latter was liable for the wrong of the security guard in doing the unlawful act under circumstances in which it ought not to have been done.

(f) *N. Sridhar* vs*. Maruthi Jayaraman and Ors*.[15]

In this case, Maruthi Jayaraman ("MJ"), the first respondent, was employed by MRF Limited ("MRF"), and had access to share certificates which were lodged for transfer with MRF. A, in the course of his employment, stole 350 (three hundred and fifty) shares lodged for transfer which came to his department with the help and connivance of other employees of MRF and prepared a forged transfer deed. MJ, subsequently, impersonating as one T. Sathyanarayana, presented the 350 shares of MRF along with the duly completed share transfer application form to the plaintiff. The plaintiff, unaware of MJ's fraud, accepted the shares for trading and placed it for sale in the market, which were subsequently sold. The sale proceeds were collected by MJ under the name of T. Sathyanarayana. However, the fraud came to light and the purchasers of the shares from the plaintiff recovered the entire amount from him. The plaintiff consequently filed a suit against MJ as well as MRF for its negligence and carelessness in failing to monitor its employee's conduct. The question before the Madras High Court was whether a company can be held to have an intention or knowledge which its agents, the officers of the company, have, and therefore, whether in the instant case, MRF was capable of forming that intention or having that knowledge and could be vicariously liable for the acts of MJ. As per the Court, it had to firstly be decided whether the employee was liable, and if yes, whether the employer had to shoulder the responsibility. The Court,

[14] 2004ACJ2020.
[15] (2009)6MLJ35.

reiterating and relying the principles of vicarious liability laid down in *Canadian Pacific Railway Company v. Leonard Lock-hart*[16], opined that if the servant at the time of accident is not acting within the course of employment but is doing something for himself, the master cannot be held liable in the eyes of law. Moreover, if the unauthorised and wrongful act of an employee is not connected with the authorised act as to be a mode of doing it, but is an independent act, the master is not responsible; as in such cases the servant is not acting in the course of the employment but has gone outside of it. Holding MRF not liable for the acts of MJ, its employee, the Court stated that when MRF came to know of the fraud committed by MJ, it had terminated MJ's services for his involvement in connection with the fraudulent and forged share transfer and had also lodged an FIR with the police, after which the fraud matter was brought to the notice of SEBI and all stock exchangers authorities. According to the Court, MJ had committed the fraud after being in possession of the documents, transfer deeds and share certificates and even though MJ was employed by MRF, MRF could not be saddled with the liability to pay the suit amount claimed by the plaintiff because misdeeds, omissions and commissions of MJ were individual, independent, personal and unauthorised, wrongful acts. Therefore, vicarious liability could not be tagged on to MRF.

5.4. *Persuasive value of English judgements in India for tort cases*

India is a 'common law country' and derives its judicial framework from the British legal system. Most of the Indian laws are based on the laws of common law countries like the United Kingdom and have been adopted with certain modifications. After India's independence, English judgements do not have binding effect in India. However, they do have persuasive effect. The Supreme Court of India has, in several decisions, including in particular the decision in *State of West Bengal* vs. *B.K. Mondal and Sons*,[17] held that whilst construing an Indian statute, it would be unreasonable to invoke the assistance of English decisions dealing with statutory provisions contained in English law. The proper course would be to examine the language of the statute to ascertain its meaning which should not be influenced by the English law upon which the statute may be founded. The Supreme Court has observed that if the words of an Indian stature are obscure or ambiguous, it may be permissible to interpret the same in light of the background of the law and English law decisions on the same.

In India, tort law remains largely uncodified. Article 372(1) of the Indian Constitution says that "*notwithstanding the repeal by this Constitution of the enactments referred to in article 395 but subject to the other provisions of this Constitution, all the law in force in the territory of India immediately before the commencement of this Constitution shall continue in force therein until altered or repealed or amended by a competent Legislature or other competent authority*". Therefore, Indian tort law is still based on pre-independence British Indian tort law, which was based on English common law.

Though Indian courts have been following English common law principles when dealing with tort law matters, there has been a drive to evolve an Indian jurisprudence in this field and the following observations of Justice Bhagwati in the case of *M.C. Mehta* vs*. Union of India*,[18] are relevant:

"*We have to evolve new principles and lay down new norms which will adequately deal with new problems which arise in a highly industrialized economy. We cannot allow our judicial thinking to be constructed by reference to the law as it prevails in England or for*

[16] AIR1943 P.C. 63.
[17] 1962 AIR 779.
[18] AIR 1988 SC 1037.

the matter of that in any foreign country. We are certainly prepared to receive light from whatever source it comes but we have to build our own jurisprudence."

Due to various inefficiencies in the Indian legal system and the extreme reluctance of Indian courts to award large amounts in damages, tort cases are few and far in between. In the absence of any Indian precedent involving an intentional, malicious and unauthorised personal data breach by an employee, we are forced examine English precedents.

5.5. *WM Morrison Supermarkets plc (Appellant)* vs*. Various Claimants (Respondents)*[19]

A recent decision by the UK's Supreme Court in the aforementioned case involves an intentional breach of personal data by an employee and the fastening of vicarious liability on the employer.

Andrew Skelton, an employee of Morrisons, during the course of his employment as an auditor in Morrison's internal audit team, downloaded and subsequently uploaded the payroll data of 98,998 employees of Morrisons on a file-sharing website. Later, he anonymously sent a cd containing the data to various newspaper outlets informing them of the data breach. The published personal details included details of salaries and bank accounts of the employees. Some of the newspaper outlets alerted Morrisons about the leak, who then took immediate action by taking down the website and contacting the police to minimise the effect of the breach. Morrisons also spent a lot of money in dealing with the aftermath of the disclosure and in protecting the identity of its employees. Skelton was convicted of multiple offences and sentenced to eight years in prison.

Subsequently, many of the affected employees brought a class action against Morrisons for its own alleged breach of the statutory duty created by section 4(4) of the Data Protection Act, 1998 ("UK DPA 1998")[20], misuse of private information, and breach of confidence. They also claimed that Morrisons was vicariously liable for Skelton's conduct. The High Court found that while Morrisons did not have direct liability under the UK DPA 1998, it was vicariously liable for Skelton's breach of statutory duty under the UK DPA 1998, his misuse of private information, and his breach of his duty of confidence. For the argument of direct liability, the High Court held that the acts of Skelton were done independently from his employer and because of that fact, Skelton became the data controller who breached the UK DPA 1998. For the contention of vicarious liability, the High Court rejected Morrison's arguments that the UK DPA 1998 excluded vicarious liability from a breach of that Act. According to the High Court, it did not matter that the breach had occurred away from the workplace or during non-working hours and there existed enough nexus between Skelton's position and his misconduct to implicate Morrisons.

The following questions arose in the appeal before the UK Supreme Court:

(a) Whether Morrisons was vicariously liable for Skelton's conduct; and
(b) Whether the UK DPA 1998 excluded the imposition of vicarious liability for statutory torts committed by an employee data controller under the UK DPA 1998, or for misuse of private information or breach of confidence.

For the first issue, the UK Supreme Court allowed the appeal and held that the lower courts had not applied the principals of vicarious liability correctly in the instant case. The Court referred to the "close connection" approach to vicarious liability laid down in the case of

[19] [2020] UKSC 12.
[20] This legislation was based on "Directive 95/46 of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data" (Data Protection Directive 95/46/EC).

Dubai Aluminium Co Ltd vs. *Salaam*[21] and held that the general principle applicable to vicarious liability arising out of a relationship of employment was as follows:

"*the wrongful conduct must be so closely connected with acts Skelton was authorised to do that, for the purposes of the liability of the employer to third parties, it may fairly and properly be regarded as done by Skelton while acting in the ordinary course of his employment*."

Under the close connection test as provided in the case of Dubai Aluminium, there were two matters to be considered; first, what functions or "field of activities" had been entrusted by the employer to Skelton; and second, whether the wrongful conduct of Skelton was so closely connected with his authorised acts that, for the purposes of the liability of his employer, it may fairly and properly be regarded as done by Skelton while acting in the ordinary course of his employment.

The UK Supreme Court held that the disclosure of the data on the internet did not form part of Skelton's functions or field of activities; it was not an act which he was authorised to do. Moreover, the mere fact that Skelton's employment gave him the opportunity to commit a wrongful act was not sufficient to warrant the imposition of vicarious liability of the employer, nor did the fact that Skelton was doing acts of the same kind as those which it was within his authority to do.

The UK Supreme Court further stated that although there was a close temporal link and an unbroken chain of causation linking the provision of the data to Skelton for the purpose of transmitting it and his disclosing it on the internet, such a temporal or causal connection did not in itself satisfy the close connection test.

Lastly, the UK Supreme Court held that the motive behind why Skelton acted wrongfully was very relevant in determining vicarious liability and the fact whether he was acting on his employer's business or for purely personal reasons was highly material. The UK Supreme Court stated ad follows:

"In the present case, it is abundantly clear that Skelton was not engaged in furthering his employer's business when he committed the wrongdoing in question. On the contrary, he was pursuing a personal vendetta, seeking vengeance for the disciplinary proceedings some months earlier. In those circumstances, applying the test laid down by Lord Nicholls in Dubai Aluminium in the light of the circumstances of the case and the relevant precedents, Skelton's wrongful conduct was not so closely connected with acts which he was authorised to do that, for the purposes of Morrisons' liability to third parties, it can fairly and properly be regarded as done by him while acting in the ordinary course of his employment." (emphasis supplied)

Thus, the UK Supreme Court held that Morrisons was not vicariously liable for the acts of Skelton.

In relation to the second issue of whether the UK DPA 1998 excludes vicarious liability for breaches of its own provisions, committed by an employee as a data controller, or for

[21] [2002] UKHL 48.

misuse of private information and breach of confidence, Morrisons argued that the provisions of the DPA impliedly excluded vicarious liability of an employer and made it clear that liability was to be imposed only on data controllers, and only where they had acted without reasonable care. It was further argued that the statutory scheme was inconsistent with the imposition of a strict liability on the employer of a data controller, whether for that person's breach of the DPA or for his breach of duties arising at common law or in equity. The UK Supreme Court held that imposing a statutory liability upon a data controller was not inconsistent with the imposition of a common law vicarious liability, either for the breach of duties imposed by the UK DPA 1998, or for breaches of duties arising under the common law or in equity.

The Court's reasoning was as follows:

"That conclusion is not affected by the fact that the statutory liability of a data controller under the DPA, including his liability for the conduct of his employee, is based on a lack of reasonable care, whereas vicarious liability is not based on fault. There is nothing anomalous about the contrast between the fault-based liability of the primary tortfeasor under the DPA and the strict vicarious liability of his employer. A similar contrast can often be drawn between the fault-based liability of an employee under the common law (for example, for negligence) and the strict vicarious liability of his employer, and is no more anomalous where Skelton's liability arises under statute than where it arises at common law."

The UK Supreme Court concluded by stating that since the UK DPA 1998 neither expressly nor impliedly indicated otherwise, the principle of vicarious liability did apply to the breach of the obligations imposed by the UK DPA 1998, and to the breach of obligations which arose at common law or in equity, committed by an employee who is a data controller in the course of his employment.

6. Conclusion

The unauthorised, malicious and intentional disclosure of the sensitive personal data by the Employee on his Facebook page was not part of the Employee's functions or field of activities. It was not an act which he was authorised or expected to do by the hospital. The Employee was not engaged in furthering the hospital's business when he committed the wrongdoing in question. It cannot fairly and properly be regarded as an act done by him while acting in the ordinary course of his employment.

Applying the tests laid down by the Indian Supreme Court in State of Maharashtra and Ors. vs. Kanchanmala Vijaysing Shirke and Ors[22], Sitaram Motilal Kalal v. Santanuprasad Jaishankar Bhatt[23], State Bank of India vs. Shyama Devi[24], Pushpabai Purshottam Udeshi and Ors. vs. Ranjit Ginning and Pressing Co. (P) Ltd. and Ors.[25], the Gujarat High Court in Anita Bhandari and Ors. vs. Union of India (UOI) and Ors.[26] , the Madras High Court in N. Sridhar vs. Maruthi Jayaraman and Ors.[27]and guided by the UK Supreme Court's

[22] (1995)5SCC659.
[23] AIR1966SC1697.
[24] AIR1978SC1263.
[25] AIR1977SC1735.
[26] 2004ACJ2020.
[27](2009)6MLJ35.

judgement in the case of WM Morrison Supermarkets plc[28], vicarious liability cannot be imposed on the hospital.

7. Recommendations

Since a malicious, intentional and unauthorised disclosure of sensitive personal data by an employee is very unlikely to be in the course of his/her employment and will most likely not be for the purpose of furthering the employer's business, there are likely to be very few situations where vicarious liability is pinned on an employer for a personal data breach by an employee. Therefore, we recommend that the PDP Bill 2019 be modified so that even if an employer is fully compliant with the law and has put in place reasonable security practices as mandated by law, the employer will still be strictly liable for and bound to compensate any data principal who suffers any loss or damage on account of a malicious, intentional and unauthorised disclosure of sensitive personal data (collected by the employer) by an employee.

As mentioned above in paragraphs 3.2.1 and 3.2.2, section 64(1) of the PDP Bill 2019 provides that any data principal who has suffered harm as a result of any violation of any provision under the PDP Bill 2019 or the rules or regulations made thereunder, by a data fiduciary shall have the right to seek compensation from the data fiduciary. The aforesaid section 64(1) also permits a data principal who has suffered harm as a result of any violation of any provision under the PDP Bill 2019 or the rules or regulations made thereunder, by a data processor, to seek compensation from such data processor, provided the data processor has acted outside or contrary to the instructions of the data fiduciary, or where the data processor was negligent, or where the data processor violated any provisions of the PDP Bill 2019. Even when a data processor is liable to a data principal, section 64 does not, technically, permit the data principal to seek compensation from a data fiduciary for the actions of a data processor which caused loss or damage to the data principal.. It is submitted that the aforesaid section 64 ought to be modified so that a claim may be made by a data principal either on the data fiduciary or on the data processor for any personal data breach caused by the data processor which resulted in loss or damage to the data principal, irrespective of whether the data processor acted as per the instructions of the data fiduciary or not. Such a provision is required since the data principal entrusted the data fiduciary with his or her personal data and the data processor was chosen by the data fiduciary. The data principal does not have a contract with the data processor and should not be forced to make a direct claim against the data processor when the data processor is at fault, though it should have the option to do so. Further, in many cases, the data processor may not have the resources to pay compensation to a data principal who has suffered loss or damage on account of the actions of the data processor.

This paper has been written by Vinod Joseph (Partner) and Deeya Ray & Protiti Basu (Associates).

[28] [2020] UKSC 12.

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 I Ahmedabad

www.argus-p.com