PROTECTING PERSONAL DATA AS A PROPERTY RIGHT

*Atul Singh**

Abstract

Personal data pertaining to a natural person is essential for a wide range of activities in the present day modern 'information society'. The importance of personal data imposes an obligation to protect personal data from unauthorised access or use and to ensure that personal data remains accurate. Protection of personal data is vital for entities which collect and process it as well as for individuals to whom this data relates. In the absence of dedicated, comprehensive data protections enactments, criminal laws with appropriate amendments, information technology laws, intellectual property laws and law of contracts are resorted to protect personal data. Another approach being considered is treatment of personal data as an incorporeal property and its protection likewise. This article deliberates on the actual and potential protection of personal data as a right in intangible property.

I Introduction

A NATURAL person is identified by his biological and biometric characteristics like appearance, height, weight, fingerprints, DNA (Deoxyrebonucleic Acid) and retinal patterns, and by acquired biographical identifiers such as address, education, driving license, passport, bank account, unique identification figures like social security number and taxation permanent account number. These identifying features form his personal information and a collection of such information is an individual's personal data. With the passage of time, developments in technology and pervading influence of electronic information, valid and verifiable personal data has become indispensable for most activities ranging from routine tasks like shopping for commonplace goods and services to critical transactions as healthcare and banking. A person lacking personal data may be denied education,[1] cellular phone service,[2] rail travel,[3] entry to the

* Ph.D. Scholar, Faculty of Law, University of Delhi. This paper is based on research work undertaken by the author for the award of his Ph.D. Degree.

[1] *Social Jurist* v. *Kendriya Vidyalaya Sangathan*, 2003 (69) DRJ 286.

[2] "(V)erification of identity proof is to be carried out before sale of postpaid/prepaid SIM cards or any kind of telephone connection.": 800-04/2003-VAS/112 on May 10, 2005, "Verification of Identity of Subscribers", Department of Telecommunications (VAS Cell), Ministry of Communications and IT, Government of India. The communique requires an applicant to provide, *inter alia* his name, date of birth, current and permanent address,

Supreme Court[4] or exercise of adult franchise.[5] As existence and use of personal data is practically unavoidable, its accuracy,[6] quality and security[7] is vital for individuals, businesses and State. A question that arises naturally is, whether personal data qualifies as property, to fall within the meaning of offences spelt out under penal statutes? In *Cox* v. *Riley*,[8] an employee erased data from a plastic circuit card. The data in the card was a computer program which controlled a computerized chain-saw which was rendered inoperable due to this erasure. The issue before the court was, whether this act could be considered as criminal damage for the purposes of the (UK) Criminal Damages Act, 1971. The English Courts have declined to recognize information *per se* as intangible property for the purposes of the Theft Act, 1968 either which consequently does not appear to be of assistance in case of misuse of information. Personal data in an unprocessed, raw form may not fit in the concept of property expounded in the general principles of criminal law. In *R.* v. *Gold and Schifreen*,[9] the respondents obtained unauthorised access to various computers in a computer network owned and operated by the British Telecommunications, by obtaining and using the customer identification numbers. They

---

proof of identity and address through income tax PAN/photo credit card/photo identity card/passport/arms license/driving license, *etc*.

3 "(U)ser is not required to give any input of the photo identity card details of any of the passengers while booking the ticket. However, he shall have to carry and show ... identity card of any of the passengers in original while travelling.": Indian Railway Catering and Tourism Corporation Ltd (IRCTC), Frequently Asked Questions, *available at* https://www.services.irctc.co.in/beta_htmls/etktfaq.html (last visited on Sep. 10, 2016).

4 "All others will have to obtain visitors' pass issued by Supreme Court Registry, for entry into the High Security Zone of the Supreme Court Premises upon proper identification.": Circular No.F. 219/Security/2007/SCA(Genl.) on May 18, 2007.

5 Registration of Electors Rules, 1960, R. 28, empowers the Election Commission of India to direct issuance of Electoral Identity Cards to electors bearing their photographs and r. 35(3) and 37(2)(b) of the Conduct of Elections Rules, 1961, in terms of which, an elector shall not be permitted to vote if he fails or refuses to produce his identity card. See also *Crawford, et al* v. *Marion County Election Board et al* 553 US 181 (2008) on Voter-ID law of Indiana, United States of America.

6 A British citizen was refused loan repeatedly and was detained at an airport having been identified as part of a dictatorial regime, based on erroneous database: M. R. McGuire, *Technology, Crime, and Justice: The Question Concerning Technomia Technology, Crime and Justice* 100 (Routledge, 2012). In *Kurien E. Kalathil* v. *Credit Information Bureau (India) Ltd*. unreported, WP(C). No. 32370 of 2007 before the High Court of Kerala, decided on Nov.19, 2008, the petitioner was aggrieved by complications arising from his name being incorrectly reported as a 'wilful defaulter' by the credit information company.

7 In what has come to be known as the 'mPhasis call centre' identity theft case, five employees of an outsourcing service provider were alleged to have used confidential information and personal identification numbers of customers to commit financial fraud by transferring funds from customer accounts to bank accounts opened using forged documents.: A. C. Fernando, *Business Ethics: An Indian Perspective* 446 (Pearson Education India, 2009).

8 [1986] Crim LR 460.

9 [1988] 2 WLR 984.

were charged with having committed forgery[10] in terms of the English Forgery and Counterfeiting Act, 1981. The House of Lords, rejecting their conviction shared the view of the Court of Appeals which had scathingly remarked the prosecution as a procrustean attempt to force the facts of the case into the language of an Act not designed to fit them. Actions under modern information technology laws brought their own dilemmas exemplified, for instance, in *Heath Cohen* v. *Gulfstream Training Academy Inc.*,[11] wherein, the respondent's information had been accessed without authorization to further a business that was competing with it. The claim was however rejected on the ground that access to information did cause an interruption of service as contemplated by the United States Computer Fraud and Abuse Act, 1986 whose language evidences intent to allow recovery for reasonable costs caused by interruptions in service or damage to a computer. A need, therefore, to explore an alternate mechanism to protect data within laws meant to protect a right in property, in a technology neutral framework, so far as possible.

Commerce has been a crucial driving force behind development of data protection laws and the difference in strategies applied by European nations and the United States(US) towards protection of personal data reflects the difference in transatlantic approach towards business regulation - larger state role in Europe whereas self-regulation based on market forces in the US. With state as the regulator of data protection and divergent national rules obstructing flow of data across borders, attempts have been made under the aegis of the Organisation for Economic Co-operation and Development (OECD),[12] the Council of the Europe[13] and the European Union (EU) to set out measures for protection of personal data applicable uniformly. Most supranational instruments recognise that personal data should not be collected or processed unless there is an unambiguous, informed consent of the person to whom the data pertains (the 'data subject'), towards such declared collection and processing. Data so collected should be proportionate to the purpose sought to be achieved by the person collecting, processing or retaining the data (the 'data controller' or 'data processor'). Collected data should be protected against unauthorised access, misuse or tampering (data security). The data subject should also

10 S. 1. The offence of forgery: A person is guilty of forgery if he makes a false instrument, with the intention that he or another shall use it to induce somebody to accept it as genuine, and by reason of so accepting it to do or not to do some act to his own or any other person's prejudice.

11 S.D. Fla., April 9, 2008, No. 07-60331-CIV.

12 Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 1980.

13 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No.108), 1981.

have a right to know his personal information in possession of a data controller and, in the event of any error, to seek a rectification thereof (individual participation, quality and accuracy). Member nations of the EU attempt to achieve this through domestic laws enacted to give effect to the European Union Data Protection Directive,[14] such as the United Kingdom Data Protection Act, 1998. The United States and some other countries lacking a comprehensive data protection enactment have been recognised by the European Commission[15] as providing adequate protection to personal data through a combination of general principles of law, enactments regulating specific areas of activity (the 'sectoral approach') and self-regulation,[16] and such mechanisms broadly recognize the same fundamental principles for protection of personal data collectively as the comprehensive European instruments.

II Sectoral protection

In the absence of any legislation with the primary object to meet the ends of data protection, personal data can be protected by laws meant to regulate specific spheres of activity involving personal data. Finance and healthcare are perhaps two sectors most intimately associated with sensitive personal information. Accordingly, legislatures have laid down the law to protect personal data managed in course of these activities. In the US, the Financial Services Management Act, 1999 commonly known as the Gramm-Leach-Bliley Financial Services Modernization Act, 1999 (GLBA) mandates privacy of personal information in the financial services sector. This Federal law is supplemented by state laws such as the California Financial Information Privacy Act, 2003. The Health Insurance Portability and Accountability Act, 1996 (HIPAA) creates standards for electronic health care transactions of health care providers, health plans, and employers, including security and privacy of medical information. The Medical Council Act, 1956 and the Dentist Act, 1948 enjoins medical professionals to maintain confidentiality of medical information in India. Confidentiality of financial information is protected under various laws such as the Reserve Bank of India Act, 1934, the State Financial Corporations Act, 1951, the State Bank of India Act, 1955, the Deposit Insurance and Credit

14 European Parliament's Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995.

15 Andorra, Argentina, Canada, Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, United States of America and Uruguay, *available at*: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm (last visited on Feb.22, 2017).

16 EU-US Safe Harbor and its replacement, the EU-US Privacy Shield, *Ibid.*

Guarantee Corporation Act, 1961, the Banking Companies (Acquisition and Transfer of Undertakings) Act, 1970 and the Credit Information Companies (Regulation) Act, 2005. Besides these laws in the financial and medical sectors, the Information Technology Act, 2000 ensures security and integrity of personal data by proscribing unauthorized access, use or alteration of electronic information resources. Computer Fraud and Abuse Act, 1986 performs a similar function in the US. While these laws maintain confidentiality, and provide some level of protection against misuse of personal data, they cannot satisfy the demands of data protection entirely, conceivably because these laws were never meant to act as data protection mechanisms and feature aspects of data protection as incidental to their main objectives. Furthermore, while these laws may assist the data protection aims of a data controller to some extent, so far as an individual data subject is concerned, elements of consent, notice, collection, use and individual participation, as referred before, are even weaker, if not altogether absent. Attempts are being made to explore the potential of protecting personal data as an incorporeal property and rights attached with such property. It should be clarified that while such rights may appear to be merely a species of well-established intellectual property rights, that would not be an entirely correct assumption, considering the objectives, ownership and rights granted under intellectual property laws as against those sought to be achieved for effective protection of personal data.

III Intellectual property rights

Information gathering and processing is a lucrative business. There are several ways and means by which personal data may be gathered and aggregated. Consequent to collection and processing, personal data takes the shape of a database. The Black's Law Dictionary defines a database as a compilation of information arranged in a systematic way and offering a means of finding specific elements it contains, often by electronic means.[17] The definition of a database being an organised collection of information held on a computer under the Oxford Dictionary of Law[18] also relates closely to automated processing of data. The ability to discover astonishing co-relations between data unrelated *per se*, using techniques such as data mining and big data analytics, reveals the knowledge power contained in large databases and underlines the need to protect such databases.

---

17 Bryan A. Garner (ed.), *Black's Law Dictionary* 452 (9th edn., Thomson Reuters, 2009).
18 Elizabeth A. Martin, *A Dictionary of Law* 134 (5th edn., Oxford University Press, 2003).

A legal right and protection of database is sought in copyright. In the United Kingdom, copyright was addressed under the Copyright, Designs and Patents Act, 1988 which had no specific provision for a database as it stood originally, though it could be considered a compilation. The European Parliament and the Council was of the opinion that either database was not sufficiently protected, or, if protected, the protection varied with national legislations across the EU . In 1996, the European Parliament and Council adopted the Directive 96/9/EC[19] for legal protection of databases. To implement the provisions of this Council Directive, Statutory Instrument 1997 No. 3032, the Copyright and Rights in Databases Regulations, 1997, was approved by a resolution of the Houses of the Parliament. These regulations give effect to the Directive 96/9/EC recognising *sui generis* right protecting databases in England and Wales. A database right exists in a database if there has been a substantial investment in obtaining, verifying or presenting the contents of the database[20] even if the work fails to satisfy the threshold of originality. A database right is, therefore, separate from, and in addition to, a copyright which may exist in a database. Regulation 16 makes extraction or reutilization of all or substantial part of a database, without the consent of the owner thereof as an infringement of database right. In *Flogas Britain Ltd.* v. *Calor Gas Ltd.*,[21] the plaintiff sought damages from the defendant for use of a database maintained by the plaintiff, containing information on its customers, their name, address, contact details, contract dates, pricing and other information. The defendant made commercial communications to the customers of the plaintiff. The High Court of England and Wales held that the information such as the names and addresses of the customers was protected by a database right and transfer of all or a substantial part of the contents of the database to another medium by any means or in any form amounted to such extraction as to constitute infringement of a database right. Under the United States Copyright Act, 1976, *Feist Publications* v. *Rural Telephone Service Co.*[22] is one of the earlier decisions on legal protection of database in the background of advances in collection, processing and distribution of information. In *Feist*, the United States' Supreme Court denied a copyrightable interest in a telephone directory produced by the defendant. The Supreme Court observed that elements of

19 Directive 96/9/EC of the European Parliament and of the Council on legal protection of databases.
20 Copyright and Rights in Databases Regulations, 1997, R. 13.
21 [2013] EWHC 3060 (Ch).
22 499 U.S. 340 (1991).

authorship in selection, coordination and arrangement of material were necessary for protection of a compilation. The court was of an opinion that originality was a constitutional requirement for protection of a compilation and while originality requirement was not stringent, there remained works that were utterly lacking in creativity and originality, as in the facts under consideration before the court. Protection of compilation of information came up for consideration of the United States Court of Appeal of for the Seventh Circuit in *ProCD, Inc.* v. *Zeidenberg*.[23] The information in question was a compilation of information from more than three thousand telephone directories into a computer database. Though it was not in doubt that the data compiled by *ProCD* was more complex, contained more information (zip codes and census industrial codes), was organized differently and was 'more original' than the single alphabetical directory at issue in *Feist*, yet it was assumed that the database could not be copyrighted. Ultimately, the plaintiff succeeded in an action on breach of contract contained in the standard form contract governing the terms of use of the software rather than a property right contained in the database. The irony of this decision is in a situation where a person having a contractual relationship with the creator of a database turns over such a database to a third-party which misappropriates information contained in a database; the creator of the database may have a cause of action against the contracting party but none *in rem* against use of the information contained in the database by subsequent parties.

A major development in India, in copyright law was the amendment to the Copyright Act, 1957 in the year 1994, to bring it fully in conformity with the provisions of TRIPS[24] Agreement. In *Burlington Home Shopping Pvt. Ltd.* v. *Rajnish Chibber.*[25] before the High Court of Delhi, the plaintiff had sought an order of permanent injunction against the defendant for copyright infringement and breach of confidentiality. The plaintiff claimed a compilation of a list of customers/database as being essential to its business and a major investment. The defendant, an erstwhile employee of the plaintiff, commenced business as a competitor to the plaintiff and was alleged to have made use of the plaintiff's said database. A defence was raised that the database was neither developed by the plaintiff nor did the plaintiff have any copyright therein. The court, however, concluded that a compilation of addresses developed by anyone devoting

[23] 86 F.3d 1447 (7th Cir. 1996).
[24] Trade Related Aspects of Intellectual Property Rights, World Trade Organization.
[25] 61 (1995) DLT 6

time, money, labour and skill amounted to a literary work wherein the author had a copyright. *Diljeet Titus* v. *Alfred A. Adebare*,[26] is often extolled as a defining moment in India on the development of copyright in a database composed of personal information; quite erroneously it may be added. The plaintiff had alleged that the defendants had been working as his employees and while leaving the employment, had made unauthorized copies of his client database over which the plaintiff allegedly had exclusive rights as the copyright owner. On the factual matrix, the case revolved around the nature of relationship between the plaintiff and the defendants and majority of the rival submissions and reasoned discussion was focussed on this aspect. The court arrived at a finding that the defendants worked for the clients of the plaintiff, the clients engaged the plaintiff's services**,** billing was done in the name of the plaintiff and the amount used to be remitted to the plaintiff. The relationships between the parties were tested on the criteria of control, ownership of tools, chance of profit and risk of loss. The court observed that copyright existed in the list of clients and addresses and that it fell within the definition of literary work within the meaning of section 2(o) of the Copyright Act, 1957 being computer database, thereby protected under copyright laws. From this foundation, the court restrained the defendants from utilizing or disseminating the data forming the subject matter of the case. An important point to consider, however, is that the database is protected by copyright as an original literary work when a modicum of skill and judgment is involved in compiling the database.[27] To that extent, the courts are not averse to applying a test of 'modicum of creativity'. Recent pronouncements from the High Court of Delhi seem to illustrate a discernible shift from a mere 'sweat of the brow' approach. The dispute in *Diljeet Titus* was not so much on existence or otherwise of copyright in client data; rather, it dealt more about ownership of such a right on the facts of that case, and, thus differentiated in subsequent decisions of the High Court of Delhi,[28] Bombay[29] and Andhra Pradesh.[30] To that extent, *Diljeet Titus* cannot be said to have laid down a proposition of law on database rights in India *per se*. On the other hand, in *American Express Bank Ltd.* v. *Priya Puri*,[31] the High Court of Delhi vacated an interim restraining order, deciding that an employee's freedom of employment cannot be curtailed on the ground of having previous

26 130 (2006) DLT 330.
27 *Vogueserv International Pvt Ltd.* v. *Rajesh Gosain,* 203 (2013) DLT 613.
28 *Stellar Information Technology Pvt. Ltd.* v. *Rakesh Kumar,* 2016 SCC OnLine Del 4812.
29 *Wits Interactive Private Ltd.* v. *Ashok Bisht*, Appeal from Order No.30904/2013 before the High Court of Bombay, order on Nov. 13, 2013.
30 *Reliability Engineering Industries* v. *Aesseal India Pvt. Ltd.,* 2013 SCC OnLine AP 480 : (2013) 6 ALD 228.
31 (2006) III LLJ 540 Del : (2006) III LLN 217.

employer's data and confidential information of customers, which was capable of ascertainment by an independent canvass at a small expense and in a very limited period of time. In *Tech Plus Media Private Ltd.* v. *Jyoti Janda*,[32] a division bench of the High Court of Delhi observed that the decisions in *Burlington Home Shopping* and *Diljeet Titus* were prior to that of the Supreme Court in *Eastern Book Company* v. *D. B. Modak*,[33] wherein it was laid down that to claim copyright in a compilation, the author must produce the material with exercise of his skill and judgment; creativity in the sense of being novel or non-obvious and not a product of merely labour and capital. The high court, in *Tech Media*, further referred to the decision of a division bench of the Court in *Akuate Internet Services Pvt. Ltd.* v. Star *India Pvt. Ltd.*[34] wherein, it was underlined that creating property (or quasi-property) rights in information stands to upset the statutory balance carefully created by the legislature through the Copyright Act. It would also be interesting to see how the courts deal with a situation where a database is compiled using automated or semi-automated computerised processing tools. Such a case may be one where a data processor collects raw data and feeds or causes to be fed raw information for compilation by an automated or semi-automated process employing computers. Neither the already existing facts are protected as an intellectual property by itself, nor the data processor can be said to have applied any 'minimal creative spark' to qualify as a protected work.

A major shortcoming of intellectual property right as a data protection mechanism is that it provides no succour to the victim of breach of data protection who simply has no *locus* in this respect. Under intellectual property laws, a data manager is under no obligation to report loss or breach of data protection. Consequently, if a data manager/controller fails to report an event of data loss or breach, the data subject would remain unaware till the time he becomes a victim of abuse of personal information; an individual is unable to mitigate the damage by taking any corrective action. A 2008 study conducted in the UK found that only 10 per cent of total marketing organizations struck by data breach considered contacting the victim.[35] Besides the

---

[32] 2014 SCC OnLine Del 1819.

[33] (2008) 1 SCC 1.

[34] MIPR 2013(3)1; MANU/DE/2768/2013 : FAO No.153/2013 before the High Court of Delhi, order on Aug. 30, 2013.

[35] "Data breach notification, in many cases, is not required by law, so it is not surprising that only 10% of marketers … report that the breach required the organization to contact the victim.": 2008 UK Study on Email Marketing Practices and Privacy, Ponemon Institute LLC, June 23, 2008 at P.5 *available at* http://www.ponemon.org/local/upload/file/StrongMail%20Email%20Research%20Report%20UK%20FINALV_7%20doc.pdf (last visited on Dec.21,2016).

costs involved in rectifying a data breach,[36] one of the motives behind non-reporting of a data breach is the indirect consequences for data manager damage to reputation and loss of business. In the 2005 study conducted by Ponemon Institute, more than 78% of those surveyed admitted that at least one, and possibly more insider-related security breaches remained unreported in their company.[37] In a survey conducted by IPOS MORI in UK , it was found that 53 per cent of the sample would immediately stop using the services of an institution which suffered a data theft. A further 48 per cent responded that they would take preventive measures and cancel all their credit cards. Also, 20 per cent of those surveyed were inclined to report a data theft event to the police as criminal matter while 17 per cent preferred to notify the relevant consumer regulatory bodies.[38] Emotional impact, which would ultimately translate into monetary loss for businesses, is indeed significant.

An intellectual property owner may not even be excessively concerned with unauthorized access to personal information as long as it does not interfere with or is in direct conflict with commercial exploitation of the rights as intended by such lawful owner. Nor do intellectual property laws prescribe any limits on use, dissemination or resale of personal information by the property rights owner himself; the laws are intended to facilitate such use, if anything. Intellectual property laws, therefore, fall short on almost all vital aspects of protection of personal data – quality, accuracy, collection/distribution/use limitation and individual participation of data subject. With its focus on commercial exploitation and near total absence of any duties on the intellectual property right owner (understandably so, considering the intent of this branch of law), intellectual property rights have a limited role in data protection.

.

IV Information property rights

Intellectual property right in a collection of personal data may not guarantee the rights of an individual data subject. Consequently, it merits consideration whether personal data by itself,

---

[36] "In a Ponemon Institute Study, "What a Data Breach Costs a Company," conducted in October 2005, it was determined that an organization's direct and indirect costs of responding to a data breach total $138.39 per data subject. These costs included the internal investigation; legal, audit and consulting services; notifications of the victims of data breach; remediation activities; and the loss of customers." – Brian T. Contoss *et al*, "The Evolution of Global Security" in Eric Cole (ed.), *Physical and Logical Security Convergence* 167 (Syngress, 2007).

[37] Brian T. Contoss *et al*, "The Evolution of Global Security" in Eric Cole (ed.) *Physical and Logical Security Convergence* 167 (Syngress, 2007).

[38] The People VS e-Commerce - Consumer Attitudes to Data Security, Secerno *available at* http://www.secerno.com/download_files/whitepapers/The_People_Vs_Ecommerce-MORI_poll.pdf (last visited on Dec.24, 2016).

in raw, unprocessed form constitutes property. The emphasis is on an inherent value in data *per se* and not as a database. Bentham has defined property as a basis of expectation of deriving certain advantages from a thing, which one is said to possess in consequence of his relation to it.[39] Brandeis considered a legal right to exclude others from enjoying property as an essential element of individual property.[40]

As far back as 1891, in *Brown Chemical Company* v. *Meyer*,[41] the Supreme Court of United States had observed that a man's name is his own property and he has the same right to its use and enjoyment as he has to that of any other species of property. Once personal information is recognized as property, the data subject has a control on use and dissemination of his personal information. Though in *Oxford* v. *Moss*[42] the High Court of Justice of England and Wales declined to treat confidential information as a form of intangible property for the purposes of the United Kingdom Theft Act, appropriation of name or likeness was classified as a privacy tort in Prosser's works.[43] According to Bloustein, the right of publicity was only a right to command commercial price for abandoning privacy and its existence depended on the fact that a name and likeness could command that price in a society.[44] The decision of the Supreme Court of Virginia in *Lavery* v. *Automation Management Consultants, Inc.*[45] was an interesting development on the issue of property right in an individual's name. The plaintiff provided consulting services for information systems and the defendant, without the plaintiff's knowledge or permission, submitted his name in a proposal to provide consulting services to the United States Navy. Relying on Code of Virginia §8.01-40,[46] Lavery sought damages for the unauthorized use of his name for trade purposes. The Court was of a view that the effect of appropriation decisions was to recognize or create an exclusive right in the individual plaintiff to a species of trade name, his own, and a kind of trademark in his likeness, though Prosser stopped short of declaring the interest protected in an appropriation case to be a property interest. The

---

39 Jeremy Bentham *et al*, *Theory of Legislation* 111-112 (Trübner and Company, 1864).
40 *International News Service* v. *Associated Press*, 248 U.S. 215 (1918).
41 139 U.S. 540 (1891).
42 (1978) 68 Cr App Rep 183 (DC).
43 William Prosser, "Privacy" 48 *Cal. L. Rev*. 383 (1960).
44 Huw Beverley-Smith, Ansgar Ohly, Agnès Lucas-Schloetter, *Privacy, Property and Personality: Civil Law Perspectives on Commercial Appropriation* 59 (Cambridge University Press, 2005).
45 S.E.2d 336 (1987)
46 Unauthorised use of name or picture of any person.

court found the reasoning in *Munden* v. *Harris*[47] applicable with equal force in *Lavery*. In *Munden*, the Missouri Court of Appeals had observed that property may consist of things incorporeal, and that things incorporeal may consist of rights common in every man. *Munden* and *Lavery* therefore make it evident that the courts were not opposed to recognize the value of personal information such as pictures and name of an individual of no singular distinction.

Competing views emerge over ownership of name and such personal information – that of the subject of personal information as its original owner having control over use and dissemination of his personal data; another view maintains that information should belong to the data collectors who have gathered personal information at the expense of time, money and effort. Yet another claim to ownership of personal data is raised on behalf of the data processors who have aggregated information into a meaningful database. Contradicting this demand is the view that such processors and database creators merely hold the personal information as trustees.[48] The latter view would conform to intellectual property based exploitation rights for database owners and yet ensure moral rights to the data subjects whose information could be considered as held by the intellectual right owner in a position of trust.

A view propounded, among others, by Kenneth Laudon, Professor of Information Systems at New York University, favours commoditization of personal information, with a property right vested in data subjects in respect of their personal data. Such model reasons for a right of data subjects to deal with their personal data for a value. Laudon posits a National Information Market and a National Information Exchange which would aggregate personal information and lease it on a regulated information market thus creating economic stakes for data processors or data controllers and data subjects.[49]

In *Vikas Sales Corporation* v. *Commissioner of Commercial Taxes*,[50] the Supreme Court of India made an elaborate analysis of the meaning of the expression 'property' referring to various dictionaries and judicial pronouncements:[51]

---

47 153 Mo. App. 652 (1911).
48 Judy Foster Davis, "Property Rights to Consumer Information", 11 *J. of Direct Marketing* 32-43 (1997).
49 Kenneth C. Laudon, "Markets and Privacy", 39 (9) Communications of the ACM, 92-104 (Sept. 1996).
50 AIR 1996 SC 2082.
51 *Id.* at 2087.

> …(T)he expression "property" has been given the following meanings … In the strict legal sense, an aggregate of rights which are guaranteed and protected by the government. … The term is said to extend to every species of valuable right and interest. More specifically, ownership, the unrestricted and exclusive right to a thing; the right to dispose of a thing in every legal way, to possess it; to use it, and to exclude every one else from interfering with it. That dominion or indefinite right of use or disposition which one may lawfully exercise over particular things or subjects. The exclusive right of possessing, enjoying, and disposing of a thing. The highest right of man can have to anything; being used to refer to that right which one has to lands or tenements, goods or chattels, which no way depends on another man's courtesy.

The court observed that the expression "property" signified things and rights considered as having money value:[52]

> Goodwill is property … as is an insurance policy and rights incident thereto … It is said to extend to every species of valuable right and interest. … This definition also shows that the expression signifies things and rights considered as having a money value.

In *Jilubhai Nanbhai Khachar* v. *State of Gujarat*,[53] the Supreme Court defined property as an aggregate of rights which are guaranteed by law. In *Chandrakant Manilal Shah* v. *CIT*,[54] while discussing the contribution of a partner of a proprietorship firm, the Supreme Court observed that like a cash asset, the mental and physical capacity generated by the skill and labour of an individual, is possessed by or is a possession of such individual. The Supreme Court remarked that in a wider sense, skill and labour were property of an individual. It may be said, though, that things that have a money value, exchangeable value, which make up wealth or which achieve a benefit for the individual may be considered as property.

---

[52] *Ibid.*
[53] 1995 Supp (1) SCC 596.
[54] (1992) 1 SCC 76 at 89-90.

To be considered as property, personal data must therefore be of some material worth for the individual. If one considers the celebrities and sportspersons, there is indeed much to be gained by endorsing and lending their names to brands. How far can an individual in India have a legal right that may be termed as a 'right of publicity'? Right of publicity is defined as a right to either prevent or to seek compensation for wrongful appropriation of one's *persona* for commercial purposes, without the consent of that person.[55] Described thus, right to publicity would appear to be a mechanism for commercial exploitation of one's name, image and likeness. Unlike a right of privacy, the right of publicity is an assignable and heritable right.[56] The subject of right of publicity was in question before the High Court of Delhi in *ICC Development (International) Limited* v. *Arvee Enterprises.*[57] The plaintiff was seeking an injunction restraining the defendant from publishing the plaintiff's logo on the defendant's advertising. The plaintiff contended that a *persona* of ICC Events vested entirely and exclusively in the plaintiff. The court, however, rejecting this contention, observed that right to personality could only inhere in an individual and not in a corporation, as under:

> The right of publicity has evolved from the right of privacy and can inhere only in an individual or in any indicia of an individual's personality like his name, personality trait, signature, voice, etc. An individual may acquire the right of publicity by virtue of his association with an event, sport, movie, etc. …
>
> Any effort to take away the right of publicity from the individuals, to the organiser {non-human entity} of the event would be violative of Articles 19 and 21 of the Constitution of India. …
>
> The right of Publicity vests in an individual and he alone is entitled to profit from it. For example if any entity, was to use Kapil Dev or Sachin Tendulkar's name/persona/indicia in connection with the 'World Cup' without their authorisation, they would have a valid and enforceable cause of action.

It is notable that in *ICC Development* case, while rejecting the claim of *persona* of a legal person, the high court referred to the existence of a right of publicity of a natural person. Indeed,

---

[55] Simon Smith, *Image, Persona and the Law* 1 (Sweet & Maxwell, 2001).
[56] *Id.* at 5.
[57] 2003 (26) PTC 245 (Del.).

the court seems to have taken a view of public figures having a valid and enforceable cause of action against the use of their personal information for commercial purposes, without their consent.

In the absence of a settled precedent, the outcome of a legal action purely on the basis of property rights in personal information is highly debatable though. In *Chandrakant Manilal Shah*,[58] practical, economic and social realities of the modern day played their role in skill and labour being considered as property; however, there do not appear to be any compelling contemporary reasons for treating personal information as property yet. Neither does there appear to be many facts in support of the society or economy recognizing substantial or uniform economic benefit from personal information, for the individual concerned. The Supreme Court has recognised an action for damages where a person's name or likeness is used without his consent, for advertising or non-advertising purpose or, in case his life story is written, whether laudatory or otherwise, and published without his consent.[59] Caution must be exercised not to confound publicity with privacy though. What the apex court intended to proscribe was unlawful invasion of privacy of the individual and not a commercial exploitation of his *persona* without his consent. The action maintainable was thus not a suit for loss of profit that could have accrued to a person by commercially exploiting his personal information; rather it was a case against invasion of the individual's privacy. Recognition of such property rights of individuals may also be resisted by the industry which generally denies the worth of raw information and, asserts that the information is of any service only after it is organized, updated and analysed by the industry.[60]

V Conclusion

Property based approach to protection of personal data is fraught with uncertainty, including, but not limited to, issues arising from costs of acquisition of data, alienability and onward transfer of property rights in data. An interesting suggestion in this regard is to balance

---

58 *Supra* note 54.

59 *R. Rajgopal* v. *State of Tamil Nadu*, AIR 1995 SC 264 at 269.

60 "There is a growing belief among consumer groups and consumers themselves that personal information is the personal property of the individual it came from. This notion of personal information as property (by which we mean information that could form the basis of a contract) has been gathering momentum as consumers become increasingly aware of their personal data in a digital economy. … In response … many businesses might argue that the customer information that they possess lacks value until it has been organized updated and analysed … Since costs are incurred to inject value into raw data, many businesses argue that they own the personal information of their customers, just like any other property or company asset." Ann Cavoukian, Tyler J. Hamilton, *The Privacy Payoff: How Successful Businesses Build Customer Trust* 93-94 (McGraw-Hill Ryerson, 2002).

competing interests in information assets akin to traditional theories of property which recognize rights in property and impose obligations owed to others arising from the ownership.[61] Property right could thus be treated as a 'bundle of rights' in the 'information property' vested as the intellectual property but qualified by legal and financial burdens associated with interests and expectations such as privacy and moral rights of other parties.[62] Personal data may also be treated as valuable property without stretching the concept to the extremes of monetisation of personal data; data subjects may be offered valuable returns such as rebates or other incentives as consideration towards permission to use their personal data for defined purposes. Such mechanism would provide some control on use of personal data to the data subject without negating the data processors expectations towards utilization of data. At the same time, data subjects preferring to retain absolute control over their personal data may refuse the use of their personal data at the cost of being ineligible for such incentives. Another aspect in commercialization of personal data emerges from the fact that living in an information society, a large portion of personal data pertaining to an individual is attributed data; *i.e.* data which has been generated by third-parties using his already existing data. Assigning value to personal data in such instances is not entirely unfamiliar. Often enough, an individual avails services free of actual costs while parting with his personal information. For instance, a person may subscribe to free e-mail service by disclosing his personal information in registering for the service. The e-mail service provider would be justified in demanding use of personal data as 'consideration' towards services provided by it and the individual is compensated in the form of free e-mail services. It is when personal information is exploited indiscriminately in such situations,[63] seeking to justify the same as a fair price for free services, that friction appears between consumers of personal data (the data controllers and processors) and consumers of services (the data subjects). What is required in such instances is the application of fair usage practises in respect of the information such that the use is known to the data subject and that certain limits

---

61 For instance, the right to own an enjoy an immovable property with a duty to maintain safety and prevent hazard to a passerby.

62 Jacqueline D. Lipton, "Information Property: Rights and Responsibilities" 56 *Florida Law Review* 135-194 (Jan., 2004).

63 "(W)e are not the customers. We instead are the products … (O)ur online behavior is captured in digital trails that are harvested by Google and Facebook to create products … And their product is the same: information. … (I)n the interests of harvesting as much information as possible, information that they analyze, tag, and sell, it serves both their interests to push privacy boundaries as far as possible … Like Google, Facebook uses the information it collects about individuals to package them up and sell them to advertisers.": Catherin Dwyer, "Privacy in the Age of Google and Facebook", IEEE Technology and Society Magazine 58-63 (Sep.2011).

are imposed on such usage and onward sharing; this could be a reasonable beginning towards responsible and mutually satisfying treatment of property contained in personal information without awaiting any final determination on absolute ownership of property rights in personal information.

Aside from any practical difficulties in establishing and maintaining a property right regime, however, there may be a fundamental opposition of this approach arising out of a consideration of protection of personal information as an inviolable, non-commercial and moral right. On a larger scale, it is contentious whether conferment or recognition of property rights in personal information, as against a right of personal dignity and integrity, is prudent at all for ensuring protection of personal data.