Christ University Law Journal
2022, Vol. 11, No. 2, 1-28
ISSN 2278-4322/https://doi.org/10.12728/culj.21.1

Intellectual Property Rights and Informational Privacy Rights: Conceptualising the Intersection for the Data Protection Regulator in India

Abhijit Rohi*

Abstract

The intellectual property regime grants exclusivity to the creator. On the other hand, data protection law aims to allow a data principal to exercise control over one's personal data. Though intellectual property law and informational privacy law may be considered two separate law domains, they have a shared history and are doctrinally, methodologically and practically still linked. In the continuing debate for establishing a data protection framework for India, the conceptual clarity about the intersection between intellectual property rights and informational privacy rights is likely to inform the choice of a framework for effectively balancing these rights. This will also be crucial in identifying and defining the role of the data protection regulator and assumes high relevance at a time when the Data Protection Bill has been withdrawn to make way for a stronger data protection framework. Against this backdrop, the paper attempts to identify how intellectual property protection and data protection intersect with each other; analyse the pre-identified challenges posed by this intersection, and the conflict

*Maharashtra National Law University, Mumbai, abhijit@mnlumumbai.edu.in; I am thankful to Ms. Shruti Dhonde, final year student at MNLU Mumbai for the research assistance provided for this article.

between the interests of the data principal and data fiduciaries. Based on the conceptualisation, the paper concludes, by proposing a suitable approach to address the challenges.

Keywords: Fundamental Right, Personal Data Protection Bill 2019, Patents, Privacy, Technology, Trade Secrets

1. Introduction

With the emergence of new technologies such as artificial intelligence, machine learning, big data analytics, deep learning, creation of neural networks, etc., the concerns surrounding privacy of a natural person, and the protection for intellectual property granted to the entities involved in developing these systems are likely to re-emerge and pose new challenges. The intellectual property regime grants exclusivity to the creator. On the other hand, the data protection law aims to allow a data principal to exercise control over one's personal data. As Megan Richardson argues, intellectual property law and information protection law can now be considered two separate areas of law, but they share a common history and remain doctrinal, methodological and practically related.[2]

In the continuing debate for establishing a data protection framework for India, the conceptual clarity about the intersection between intellectual property rights and informational privacy rights will likely inform the choice of framework for effectively balancing these rights. Consequently, this conceptual clarity may help guide the actions of the future data protection regulator. In a data-driven world, more often than not, personal data of data principals is used as raw material in developing systems capable of

[2] Megan Richardson, Handbook of Intellectual Property Research: Lenses, Methods, and Perspectives (Irene Calboli et al. eds, 2021).

impacting human lives both positively and negatively. The data protection framework is used as a tool to advance the positive impact and to minimise the negative consequences. Accordingly, if harm to privacy is to be considered a negative consequence, a data protection framework is aimed at preventing harm to privacy. If the harm has accrued, it provides remedies to the data principal for the same.

There are multiple rights which are bundled together as informational privacy rights. These include, right to confirmation and access, right to correction and erasure, right to data portability, right to be forgotten, right to file complaint and right to seek compensation - together they form the core rights of the data principal in a data protection regime. The present paper focuses on two of these rights namely, right to confirmation and access and right to data portability. The expression informational privacy rights in the context of the present paper may be construed accordingly. The decision to focus on these two rights is a considered one. As these rights, unlike others (barring right to be forgotten[3]) are capable of impacting intellectual property rights. Similarly, the expression 'intellectual property rights', for the purposes of present paper include legal protection of copyright, trade secrets and patents (to a limited extent permissible under the Indian patent law).

The need for having legislation for protection of informational privacy in India has been suggested by various committees constituted by the government and also numerous scholars. The adoption of comprehensive legislations for data protection has been followed as a trend in the majority of countries. A group of experts to deliberate on privacy issues, under the

[3] Ankita Aseri, Juxtaposing right to be forgotten and Copyright Law, 25 JIPR 100-104 (2020).

chairpersonship of Justice A. P. Shah was constituted by the Planning Commission of India in 2011. The group of experts in its report [4] recommended adoption of National Privacy Principles after engaging in the comparative analysis of the international privacy principles. For the purpose of creating regulatory framework for privacy, it recommended that a 'Privacy Act' should create a regulatory framework for both public and private sector organisations. The establishment of the offices of 'Privacy Commissioners at central and regional levels, where the Central Privacy Commissioner is accountable to the parliament and all privacy commissioners to have powers to receive and investigate any complaint, was also recommended. The other prominent governmental initiative was constituting a committee of experts under the chairpersonship of Justice B. N. Srikrishna, Former Judge, Supreme Court of India[5] 'to study various issues relating to data protection in India and to make specific suggestions on principles underlying a data protection bill and draft such a bill.'[6] Accordingly, the Committee issued a 'White Paper of the Committee of Experts on a Data Protection Framework for India' [7] in November 2017 and subsequently submitted its Report[8] along with the draft Personal Data Protection Bill, 2018 ('the Bill'). [9] The Bill, 2018, proposed establishing a Data Protection Authority of India.

---

[4] Report of the Group of Experts on Privacy Planning Commission, Government of India (2012).

[5] CLES for Constitution of a Committee of Experts to deliberate on a data protection framework for India, MEITY Government of India, Office Memorandum No. 3(6)/2017 (2017).

[6] *id*.

[7] White Paper of the Committee of Experts on a Data Protection Framework for India (2019).

[8] A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians, Committee of Experts under the Chairmanship of Justice B. N. Srikrishna, MEITY, Government of India (2019).

[9] The Personal Data Protection Bill (2018).

On December 11, 2019, the Personal Data Protection Bill, 2019 (hereafter referred to as the Bill 2019) was introduced in the Lok Sabha by the Minister of Electronics and Information Technology, Government of India. The Bill, 2019 also proposed that the Data Protection Authority of India is to be established by the Central Government.[10] However, the said Bill was heavily objected to, because of the broad powers which were proposed to be conferred on the government. In light of the heavy criticism of the Bill, in 2019, a Joint Parliamentary Committee ('the JPC') was constituted to consider the objections through a long consultative process of the stakeholders.[11] The JPC released its report along with the text of the Personal Data Protection Bill, 2021 ('the PDP') on Dec. 16, 2021.[12] However, on Aug. 3, 2022, the Ministry of Electronics and Information Technology, Government of India, withdrew the PDP Bill, 2019 in the light of JPC's proposal of 81 amendments and 12 recommendations and proposed to introduce a new, comprehensive bill.[13] Even though the PDP Bill, 2021 has been withdrawn, the efforts leading to its introduction and withdrawal provide a strong jurisprudential foundation for India's data protection regime in the future. These efforts were to establish an independent, expert and sector-agnostic data protection regulator. The primary

[10] cl. 41, The Personal Data Protection Bill, 2019.

[11] The committee was constituted on Dec. 11, 2019. The details about the committee are available at http://loksabhaph.nic.in/Committee/CommitteeInformation.aspx?comm_code=73&tab=1, (last visited on June 21, 2022).

[12] Report of the Joint Committee on The Personal Data Protection Bill, 2019, Lok Sabha, Government of India (2022).

[13] Soumyarendra Barik, *Govt Withdraws Data Protection Bill to Bring Revamped, Refreshed Regulation*, THE INDIAN EXPRESS (Aug. 4, 2022) available at https://indianexpress.com/article/india/government-withdraws-data-protection-bill-8068257/, (last visited on Aug. 4, 2022).

objective of all future data protection regimes is likely to establish such a data protection regulator in India.

Both the Joint Parliamentary Committee and Justice B. N. Srikrishna Committee had considered the issues of the intersection between informational privacy rights and intellectual property rights. However, their recommendations are contradictory. There is a need to revisit the rationale for such contradictory recommendations and to establish an approach to be followed by the proposed data protection regulator.

In this backdrop, the paper is divided into five sections. The introductory part traces the developments in the domain of data protection in India to set the grounds for further engagement, the subsequent part focuses on identifying how intellectual property protection, and data protection intersects with each other. It looks at copyright protection, trade secrets protection and patent protection in the domain of emerging technologies. The next part identifies the challenges posed by this intersection. It focuses primarily on the right to confirmation and access and the right to data portability of the data principal. Additionally, the conflict between the interests of the data principal and data fiduciaries are highlighted. The concluding part analyses and proposes a suitable approach to address the challenges. Recognising the social value of informational privacy protection, the nature of data and challenges for its control are analysed before proposing the role of a data protection regulator in responding to these challenges.

2. The Intersection of Intellectual Property Protection and Data Protection

There are certain aspects which prominently highlight the intersection of intellectual property protection and data protection. This part engages in the identification and

exploration of three of these aspects, viz., protection of databases under the copyright regime, protection of trade secrets, and grant of patents in the domains of emerging technologies. Duplication raises concerns because the intellectual property protection so granted involves personal data. Data are, therefore, the basis of databases and their protection under the copyright system. Trade secrets protect how data is collected and processed, and new technologies like artificial intelligence and machine learning are data-driven.

A. Copyright Protection of Databases

Intellectual property rights and informational privacy rights have been historically intertwined. Doctrines such as an author's right to first publication and the doctrine of breach of confidence were instrumental not only in copyright law and the law on trade secrets, but also in protecting the informational privacy of an individual.[14] Further, intellectual property rights are justified by the Personality theory. According to the Personality theory, "intellectual property is an extension of individual personality". [15] Informational privacy rights are also "an aspect of inviolate personality".[16] Hence if the legitimate expectation from copyright protection is that the work protected by the copyright remains in the exclusive control of the author of the copyright, the legitimate expectation from the right to informational privacy vis-à-vis intellectual property protection must be that the data principal retains exclusive control over one's personal information. Such

[14] Supra note 1.

[15] Adam Moore, and Ken Himma, Intellectual Property, Stanford Encyclopedia of Philosophy (Fall 2022 Edition), Edward N. Zalta & Uri Nodelman (eds.), available at https://plato.stanford.edu/archives/fall2022/entries/intellectual-property/, (last visited on Aug. 19, 2022).

[16] Supra note 1.

exclusive control of the data principal over her information is fortified by the fundamental right to privacy.

A database is "a collection of independent works, data or other materials arranged systematically or methodically and individually accessible by electronic or other means."[17] In the European Union, databases enjoy two-fold protection, first, "copyright protection for the intellectual creation involved in the selection and arrangement of materials";[18] and second, "*sui generis* protection for a substantial investment…in obtaining, verifying or presenting the contents of a database."[19] The author, i.e., the creator[20] of a database in the EU, is granted exclusive rights with respect to the display, distribution, reproduction, alteration and performance of the database to the public.[21] In India, there is no specific legislation protecting databases. However, the protection is interpreted to be available under a few legislations, such as Indian Contract Act 1872, Copyright Act 1957 and the Information Technology Act 2000. Copyright protection is available to a database based on the labour and investment in collecting, compiling, organising and presenting the data in a specific format.[22] In *Eastern Book Company* v. *D.B. Modak*[23], the Supreme Court held that a compilation can enjoy copyright protection as long as it is original and "originality requires only that the author makes the selection or arrangement independently and that it

[17] Directive on the Legal Protection of Databases, European Parliament and of the Council, 96/9/EC, at 20-28 (1996).

[18] *id.*

[19] *id.*

[20] *id* at art 4.

[21] *id* at art 5.

[22] V. Govindan V. E.M Gopalakrishna, AIR 1955 Mad 391; Burlington Home Shopping V. Rajnish Chibber, 61 (1995) DLT 6; The Himalaya Drug Company V. Sumit 126 (2006) DLT 23; Eastern Book Company V. D.B. Modak, (2008) 1 SCC 1.

[23] Eastern Book Company V. D.B. Modak, (2008) 1 SCC 1.

displays some material with a minimal level of creativity."[24] Even the data in the public domain can enjoy copyright protection if selected and arranged as a distinguishable database. Accordingly, the threshold is a compilation depicting even a 'modicum of creativity'.

A database may consist of the personal information of individuals. Data sets created and used for processing by the data fiduciaries or processors may contain sensitive personal information of the data principals. Such compilation of information is protected under copyright law.[25] However, personal and sensitive personal information, as defined under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules, 2011)[26] under the Information Technology Act, 2000, have notions of privacy associated with it and accordingly, any database containing such information is subject to the protection of SPDI Rules, 2011 and Section 66E of the Information Technology Act, 2000.

B. Protection of Trade Secrets

A trade secret can be identified as information that, *first*, is a secret, in that "it is generally known among or readily accessible to persons within the circles that normally deal with the kind of information",[27] second, reasonable steps have been taken to keep it a secret, and lastly, it has commercial value.[28] Information collected by commercial as well as non-

[24] Eastern Book Company V. D.B. Modak, (2008) 1 SCC 1.

[25] Diljeet Titus v. Alfred A. Adebare, 2006 (32) PTC 609 (Del); in EU, Flogas Britain Ltd. v. Calor Gas Ltd., [2013] EWHC 3060 (Ch).

[26] Rule 2(1)(i) and Rule (3), The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

[27] Agreement on Trade-related Aspects of Intellectual Property Rights, art 39(2), 1995.

[28] *id*.

commercial institutions, including "information on customers and suppliers,…and market research and strategies" [29] can constitute a trade secret.[30]

The primary challenge posed by the intersection of intellectual property and informational privacy is that the information that is protected as intellectual property is personal information of individuals who do not enjoy intellectual property rights over their own information. It is the author of the database or the owner of the trade secret who is empowered with exclusive economic rights in terms of display, distribution, alteration, reproduction and presentation of the data. Hence, the data principal, i.e., individuals whose information under the intellectual property rights, are granted to a third person, lacks control over their data regarding its storage, transfer, usage and safety. Although such individuals enjoy a right to informational privacy, there are no suitable exceptions to the discussed intellectual property rights on the grounds of informational privacy. Therefore, demarcating the domain of intellectual property rights to the point where it meets informational privacy, and consequently, limiting intellectual property rights to provide for informational privacy, is the key challenge.

This challenge aggravates in the contemporary world where the internet and social media have become a necessity, where individuals are effectively compelled to consent to the standard terms of service of the service provider, to avail a

[29] Directive on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, European Parliament and of the Council, (EU) 2016/943, (2016).

[30] Banterle, Francesco, The Interface between Data Protection and IP law: The Case of Trade Secrets and Database Sui Generis Right in Marketing Operations, and the Ownership of Raw Data in Big Data Analysis (2016). PERSONAL DATA IN COMPETITION, CONSUMER PROTECTION AND INTELLECTUAL PROPERTY LAW TOWARDS A HOLISTIC APPROACH?, (Bakhoum, M., Conde Gallego et al. eds., 2016).

service.[31] Hence, on account of a lack of bargaining power, individuals are compelled to provide their personal information to entities who collect, process and effectively control their personal data. As discussed above, since these entities enjoy intellectual property protection not only for the processing of the data but also for the data itself, they do not owe transparency and accountability to the data principals. Therefore, data principals not only lose control over their data but also forego any right to economise their exclusive rights over their personal data for fear of being subjected to an infringement action.

C. Patents protection in the domain of emerging technologies

New forms of technologies such as artificial intelligence (AI), big data analytics, machine learning, internet of things (IoT), deep learning, artificial neural networks etc., are constantly emerging. India also promotes innovation in the AI sector. Technological advancements are granted intellectual property protection. According to a July 2021 research Report of INDIAai and NASSCOM, 'India is emerging as a key destination for AI innovation'; the technology sector has filed the most AI patents, and the trend is likely to maintain an upward trajectory.[32] There are some documented concerns over the development and deployment of AI. These include, but are not limited to concerns over data privacy, including tracking and individual profiling, data security, data biases and data quality.[33] These data-driven advancements are likely

[31] Simon Geiregat, Copyright Meets Consumer Data Portability Rights: Inevitable Friction between IP and the Remedies in the Digital Content Directive 71(6) GRUR International (2022).

[32] AI Patents: Driving Emergence of India as an AI Innovation Hub, NASSCOM, SAGACIOUS IP, INDIAAI (June 2021).

[33] Consultation paper Leveraging Artificial Intelligence and Big Data in Telecommunication Sector, TRAI, at 76-82 (2022).

to pose new forms of challenges to the intersection between intellectual property protection and data protection.

3. Challenges posed by the intersection

The interaction between intellectual property rights and informational privacy rights can generate conflicts. When the intellectual property rights of one person threaten the informational privacy rights of the other, a conflict between the two is bound to arise. The following part carves out two such challenges. First, there is a possibility that IP protection may act as an obstacle in exercising two informational privacy rights, viz. right to access and confirmation and the right to data portability. Second, the need to balance the manner of protection of these competing interests.

A. IP Protection as an impediment in exercising informational privacy rights:

1. Right to access and confirmation

The right to confirmation and access is a combination of two interests of the data principle. These interests include, *first*, an interest in being informed about the status of processing one's personal data and *second*, an interest in being informed about the other details, such as the purpose of retention, processing etc., of one's personal data available, with a data fiduciary along with the information about the processing activities undertaken. Broadly, the first interest relates to the right to confirmation and the second interest to the right to access. The purpose of the right to confirmation and access is to inform the data principal about the details and status of one's personal data. The right to confirmation and access is a right of a data principal to inquire regarding the processing of one's personal data and to gain access to one's personal data, which is available with the data fiduciary. This right is aimed at giving effect to the 'individual participation principle', which ensures

that the data principal has to ability to influence the processing of one's personal data.[34]

As per the Bill, 2019, the right to confirmation and access is proposed to be available to every data principal. [35] Accordingly, the data principal has a right to obtain three kinds of details from the data fiduciary, namely, the confirmation about the status of the processing of personal data by the data fiduciary; *second*, the personal data of the data principal or its summary; third, a brief summary of processing activities undertaken by the data fiduciary including any information provided as part of the notice requirement[36] for such processing. [37] It also proposes to mandate the data fiduciary to provide this information in a clear, concise manner which is easily comprehensible to a reasonable person.[38] The Bill, 2019 introduces an additional component to the right to access by mandating that the data fiduciary must provide details of the third parties with whom the personal data of the data principal is being shared, along with the details of the categories of personal data shared with them.[39] The scope of this right and the actions that are required on the part of the data fiduciary may raise concerns over copyright and trade secrets protection. The data fiduciaries may claim that they have intellectual property rights in the information they generate. The trade secrets related challenges are discussed below in the context of the right to data portability.

[34] *Supra* note 6 at 122.
[35] *Supra* note 9 at cl. 17.
[36] *Supra* note 9 at cl. 7.
[37] *Supra* note 9 at cl. 17(1).
[38] *Supra* note 9 at cl. 17(2).
[39] *Supra* note 9 at cl. 17(3).

2. Right to data portability

This is yet another right proposed to be conferred on data principals in India empowering them to exercise control over their personal data. This right also stems from the principle of individual participation in the data protection regime. This right facilitates the ability to move, copy or transmit personal data easily from one data fiduciary to another[40] and is critical in making digital economy seamless. [41] Allowing data principals to obtain their personal data available with any data fiduciary, empowers them by granting greater control over their own personal data. Additionally, by allowing data principals to transfer their personal data from one data fiduciary to another, the free flow of data is facilitated. Which improves competition between fiduciaries and therefore, has the potential to increase consumer welfare.[42] However, it is a qualified right.

In the EU, there are two distinct rights recognised under a right to data portability viz. the right to receive the personal data in a commonly used machine-readable format, and the right to transmit personal data from one organisation to another, where it is technically feasible.[43] The Bill 2019 also proposes to incorporate these two rights.[44] The first right is the right to receive personal data in a structured, commonly used and machine-readable format[45] and second, right to have personal data transferred to any other data fiduciary.[46] However, this is only with respect to the data, provided to the data fiduciary by data principal. The data which has been generated in the

[40] *Supra* note 6 at 131.

[41] *Supra* note 7 at 75.

[42] Paul de Hert et al., *The right to data portability in the GDPR: Towards user-centric interoperability of digital services*, 34(2) COMPUTER LAW & SECURITY REVIEW 193-203 (2017).

[43] Article 20(1), *The GDPR*.

[44] *Supra* note 9 at cl. 19(1).

[45] *Supra* note 9 at cl.19(1)(a).

[46] *Supra* note 9 at cl.19(1)(b).

course of business by the data fiduciary or the data which forms part of any profile on the data principal, or which was otherwise obtained by the data fiduciary, can be neither received nor sought to be transfer of by the data principal.

As the right to data portability is a qualified right, there are two major limitations explicitly laid down by the Bill 2019.[47] First, the right is not available if the processing of such data is necessary for functions of the State or in compliance of law or order of a court.[48] Second, as the personal data generated in the course of business can be received by the data principal by exercising this right, it is possible that such information could reveal trade secrets of the data fiduciary. The right is qualified if the data received by the data principal 'would reveal a trade secret of any data fiduciary or would not be technically feasible'.[49] Thus, a request obtaining the data may be denied if it is impossible to provide the information without revealing trade secrets.

The Srikrishna Committee Report mentions the utility of the right to data portability 'in making digital economy seamless'.[50] This right grants more control to the data principal over one's data even when one has shared the same with data fiduciaries. Without advancing any direct rationale, the Report claims,

> As the right [to data portability] extends to receiving personal data generated in the course of provision of services or the use of goods as well as profiles created on the data principal, it is possible that access to such information could reveal trade secrets of the data fiduciary. To the

[47] *Supra* note 9 at cl.19(2).
[48] *Supra* note 9 at cl.19(2)(a).
[49] *Supra* note 9 at cl.19(2)(b).
[50] *Supra* note 41.

> extent that it is possible to provide such data or profiles without revealing the relevant secrets, the right must still be guaranteed. However, if it is impossible to provide certain information without revealing the secrets, the request may be denied.[51]

However, elsewhere the Report acknowledges that the right to privacy is to be enjoyed by the natural persons, the same cannot be advanced to the juristic persons as other forms of protection are available to them in the form of intellectual property rights, contractual rights etc. [52] Accordingly, the Committee has subjected the fundamental right to privacy (informational privacy being a facete of it[53]) of data principals to intellectual property protection of trade secrets of the data fiduciaries and data processors. The PDP Bills 2018 and 2019 both included revealing of trade secrets as an exception to data principal's exercise of right to data portability.[54]

In Indian context there is limited clarity on what constitutes trade secrets and how are they to be a part of protected intellectual property. [55] In this backdrop, the Department Related Parliamentary Standing Committee on Commerce presented the 161st Report on 'Review of the Intellectual

---

[51] *Supra* note 41.

[52] *Supra* note 7 at 25.

[53] Justice K. S. Puttaswamy (Retd.) and Ors. v. Union of India and Ors., (2017) 10 SCC 1.

[54] *Supra* note 8 at cl. 26; *Supra* note 49.

[55] See, Burlington Home Shopping Pvt. v Rajnish Chibber, MANU/DE/0718/1995; American Express Bank Ltd. v Ms. Priya Puri, MANU/DE/2106/2006; Indiana Gratings Private Limited and Ors v Anand Udyog Fabricators Private Limited and Ors, ANU/MH/1465/2008; Tania Sebastian, *Locating Trade Secrets under Indian Laws: A Sui Generis Mode of Protection*, 27(3) JIPR 202-211 (2022).

Property Rights Regime in India' on July 23, 2021.[56] The Report while, *first*, making reference to the National IPR Policy and *second*, also noted the inadequacy of the existing regime in protecting trade secrets recommended 'enacting a separate legislation or a framework for protection of trade secrets'.[57]

Accordingly, the Joint Parliamentary Committee (JPC) in its re-examination of the scope of the exceptions to right to data portability, observed that, trade secrets is a dynamic concept and the same cannot be defined in the Bill for data protection and that it provides disproportionate scope to data fiduciaries to conceal their actions under the garb of protection of trade secrets.[58] These observations of the JPC are pro-protection of informational privacy and recognise the supremacy of the informational privacy rights of the data principals over intellectual property rights of the data fiduciaries.

B. **The Competing Interests**

The foregoing analysis suggests that in certain contexts, intellectual property protection and informational privacy protection may come in conflict with each other. The need is to resolve such a conflict and effectively balance these interests. The balancing exercise may be characterised by combination of the two approaches. This can be done first by resorting to the already existing provisions under the statutes providing IP protections and secondly, by creating a conceptual framework for addressing the challenges, emphasising on the role of the data protection regulator. This subpart focuses on the first

[56] Review of the Intellectual Property Rights Regime in India, Department Related Parliamentary Standing Committee on Commerce, Rajya Sabha, Parliament of India, 161 (2021).

[57] *Id*. at 79-81.

[58] Report on The Personal Data Protection Bill, 2019, Joint Committee, Lok Sabha, GoI at 78 (2021).

approach and the following part deals with the latter approach.

Both the Copyright Act, 1957 ('Copyright Act') and the Patents Act, 1970 ('Patents Act') contain provisions for minimising the negative effects of the exclusivity conferred on the author or the inventor as the case may be. Provisions like fair use[59] and fair dealing in case of copyright and section 3 along with compulsory licencing[60] in case of patents have established strong jurisprudential foundations for balancing individual centric IP protection and larger public interest. In the Chancellor, Masters and Scholars of the *University of Oxford v. Rameshwari Photocopy Services and Ors*.[61] the Delhi High Court while referring to the Indian social realities has interpreted section 52 of the Copyright Act to advance larger public interest as opposed to the private commercial interests of the publishers. Additionally, "any invention the primary or intended use or commercial exploitation of which could be contrary to public order or morality or which causes serious prejudice to human life" is a non-patentable invention.[62] Similarly, the provisions for compulsory licensing are meant for protecting and advancing larger public interest by issuing licenses to work the invention without the consent of the intellectual property rights' owner if the owner has been misusing the exclusivity without regard to the public at large. These provisions and their underlining jurisprudence provides clarity in balancing the interests in the event of conflict between an intellectual property rights' owner's individual commercial interests on the one hand and interests of the general public at large, on the other. The utilitarian theory justifies the protection of intellectual property as it encourages

[59] s.52, the Copyright Act, 1957.

[60] *ibid* at s.100.

[61] University of Oxford v. Rameshwari Photocopy Services and Ors.,235 (2016) DLT 409.

[62] *Supra* note 61 at s.3(b).

"optimal amount of intellectual works being produced, and a corresponding optimal amount of social utility".[63] Hence, social utility is the end and intellectual property rights are the means.

Collection and use of the personal data of the data principals by the data fiduciaries to advance their own economic interests in the data-driven economy, amounts to treating the data principals as mere means to an end. Kant philosophises human beings as an end in themselves rather than as a means to an end. This calls for respecting the inherent worth of human beings instead of using them as means to derive something of worth.[64] Treating human beings as means in this manner amounts acting in contravention to the fundamental right to privacy guaranteed to individuals.

Additionally, balancing these competing interests become even more challenging since promotion of innovation by conferring adequate intellectual property protection contributes to economic development. A stricter regulation in favour of informational privacy protection is opposed by the data fiduciaries and processors on the ground that compliances are economically burdensome and may lead to a negative impact on market competition. Even though these challenges exist, there is a need to conceptualise a model in order to effectively deal with this intersection.

4. Deciding the suitable approach to address the challenges

Following the identification and analysis of the challenges posed due to the intersection, in the previous section, this section aims to conceptualise a suitable approach for addressing these challenges. Accordingly, this part is divided

[63] Intellectual Property, Stanford Encyclopaedia of Philosophy (2022).
[64] The Humanity Formula, Kant's Moral Philosophy, Stanford Encyclopaedia of Philosophy (2022).

in three sub-parts. The *first* sub-part analyses the larger public interest involved in the protection of informational privacy. The second sub-part argues for understanding the nature of data and challenges in exercising control over it. Lastly, the role of the data protection regulator is conceptualised as an independent expert requiring the abilities to oversee the impact of use of technology on informational privacy, to seek co-operation from other sectoral regulators to effectively address the intersection.

A. Recognising the social value of informational privacy protection

Data protection emanates from the right to privacy. Privacy as a concept has various contours. In order to understand the intersection, privacy needs to be established as an interest worth protecting. There are various reasons which have been identified as conferring significant value to privacy. Privacy promotes psychological well-being and is essential for self-development. It creates space for intimate relationships and is important for democracy's success. At the same time, there are some reasons which have been identified for not protecting privacy. Privacy is viewed as a threat to community and solidarity. Privacy impedes social control. Privacy protection is detrimental to building trust and evaluating a person's reputation. Privacy can impede commercial efficiency and profitability. It also conflicts with the free flow of information. The concept of privacy emerges from autonomy and liberty, and it has constantly been pointed out that the protection of privacy cannot be absolute.[65] This implies the following:

1. Privacy is not absolute rather it is qualified.

[65] Supra note 53.

2. In the event of a conflict between privacy and some other valuable social good, which prevails, will always be an act of comparative assessment.

Therefore, there is a need to find the balance between these competing claims. The act of balancing is a matter associated with privacy valuation.

The consequentialist accounts of privacy valuation suggest that while determining the value of privacy one has to look at the ends that privacy protection will advance. The following questions may provide some guidance for an account of privacy valuations:

1. What is the interest that is being advanced by the protection of privacy?
2. How much importance is associated with the interests being advanced?
3. What is the reasonably perceived effect on other valuable interests in the absence of privacy protection?

The consequentialist account of privacy valuation has three major implications. First, if there is no negative effect of the absence of privacy protection on any other interest and the privacy protection itself is not advancing any other valuable interest, privacy protection is not considered viable. Second, it bases itself on the presumption that privacy protection does-not have intrinsic value. And third, privacy is valuable only with reference to some other interests. On the other hand, the non-consequentialist accounts of privacy valuation are based on the presumption that privacy is intrinsically valuable. By virtue of being human beings, we all have a moral duty to respect an individual's dignity, liberty and autonomy. A threat to privacy appears to threaten the integrity of a person, and thus from a Kantian notion of recognising persons as ends, it is

forbidden to override a person's fundamental interests for the purpose of maximising the happiness for all.[66]

While determining the value of privacy the other consideration is the manner in which privacy is framed. Is privacy to be considered a mere individual right or should it be considered as having larger social value? If privacy flows from the concepts of individual autonomy, liberty and dignity, the probable consequence is privacy being perceived as merely an individual right. Individualistic construction of privacy assumes significance also because of the interests which are perceived as conflicting with privacy such as freedom of speech and expression, right to information, national security, prevention and investigation of crimes etc., which are perceived in terms of their larger social value. However, the fact that privacy is an individual right may not necessarily exclude the larger social value of protection of privacy. It has been observed that formulation of privacy as an individual right undervalues its significance in social life. There are multiple interests which are advanced by privacy protection and most of these interests are significant from a social angle. Thus, as discussed in the previous section, if the larger public interest is to take precedence over intellectual property owner's individual commercial interest then the same principle has to be adopted while addressing the conflict between intellectual property protection and informational privacy protection since informational privacy protection serves to advance the public interest.

Understanding the Nature of Data and challenges for its control

Some of the characteristic features[67] of the information in an online environment are:

---

[66] Charles Fried, *Privacy*, 77 Yale L.J. 475, 482 (1968).

[67] *Supra* note 53.

1. Information is non-rivalrous, implying that the same information can be simultaneously possessed and consumed by multiple consumers;
2. Information is invisible, implying that there is no tangible form in which information and its possession can be defined;
3. Information is recombinant, implying that information as an output can be used as an input for further information generation.

This nature of information has posed challenges to the traditional legal regime primary focused on the protection of rivalries and tangible form of property. The information collected can be used for multiple purposes. An output once derived with the use of information and its processing subsequently can be used as an input for further information processing to reach different conclusions and output. Also, electronic tracks contain powerful means of information which provide behavioural knowledge of the user. Additionally, it must be noted that the information available on the internet is permanent in nature. The incidences in real life may be forgotten by the human mind, however, the internet poses a new challenge by making the recording of the information a norm. Clinging on to the activities in the past of a person does not accord an opportunity to reinvent and reform themselves. Human progress is marked by an individual's ability to bring changes in one's behaviour and beliefs. Personal evolution and reformation are possible in a society which provides opportunities to forget past mistakes and to not let the past determine the present and future of an individual. Since every activity of an individual is tracked on the internet, the records grant permanency to such activities.

With the changing nature of technology, it is increasingly difficult to determine the severity or the risk of privacy harm.

In order to effectively protect the rights of the data principal, the emphasis on precautionary measures has to be higher. The emerging technologies are blurring lines between personal data and sensitive personal data. In this context, due to the recombinant nature of information, the data breach or privacy harm may cause irreparable damage to the data principal. Personal data once compromised may have a rippling effect on the informational rights of the data principal which consequently, undermines the fundamental right to privacy.

The grant of intellectual property protection to the innovations or technical developments in the domain of emerging technologies, as discussed before, may be as patents, copyright or trade secrets, result in granting exclusivity to the data fiduciary or data processor. However, can the technologies developed based on the data gathered from data principals for which exclusivity is conferred on the data fiduciaries also exclude the data principals themselves?

With the emergence of new forms of technologies, new challenges are also emerging. Combination of these technologies with above mentioned nature of data is going to be a further cause of concern for informational privacy protection. There are various initiatives being taken to ensure that emerging technologies are ethical. The developments of concepts such as trustworthy AI, responsible AI, explainable AI, etc., are illustrative of the such concerns. In India, two documents focusing on 'Principles of Responsible AI'[68] and 'Operationalizing Principals of Responsible AI' [69] were published by NITI Aayog in February and August 2021 respectively. The European Union's 'Ethics Guidelines for Trustworthy AI' released in April 2019, enlists respect for privacy and data protection as one of the guidelines along with

[68] Responsible AI #AIforAll, Approach Document for India, Part 1- Principles of Responsible AI, NITI Aayog (2021).

[69] Responsible AI #AIforAll, Approach Document for India, Part 2- Operationalizing Principles of Responsible AI, NITI Aayog (2021).

auditability of AI systems as part of the accountability requirements.[70] In the case of development, deployment and use of AI systems the issues about balancing the informational privacy rights and intellectual property rights arise. The auditability under EU Guidelines though entails undertaking an assessment of AI systems, there is no need to have information about intellectual property about AI systems available publicly. However, if the AI systems are affecting the fundamental rights, then the systems must be independently audited. Such a model is respectful of the intellectual property rights and informational privacy rights.

B. Role of the Data Protection Regulator

The primary task of the data protection regulator is to protect informational privacy of data principals. The data protection authority is designed as protector and promoter of interests of all the stakeholders namely data principals, data fiduciaries, data processors while channeling research and developments in the domain of information technology in a privacy-conscious manner. It also has the responsibility to put systems and processes in place in order to provide an opportunity to - realise and enforce the rights of data principals. This entails, sometimes not only engaging in monitoring and supervising data fiduciaries and data processors but also working with them to achieve the desired objective of informational privacy protection. Data principal as an individual does not have the ability, financial or otherwise, to effectively question the functioning of the data fiduciaries and processors.

With growing concerns over privacy invasion in the light of recent experiences such as Cambridge Analytica data

[70] Ethics Guidelines for Trustworthy AI, The High-Level Expert Group on AI, European Commission, (April 2019).

scandal,[71] and the Uber data breach,[72] the data principals do not view the conduct of data fiduciaries as trustworthy. Exclusivity conferred by intellectual property protection on the data fiduciaries or data processors ought not to infringe upon informational privacy rights of an individual.

The transparency and accountability obligations proposed to be imposed on the data fiduciaries shall supersede IP protection in the event of breach of informational privacy rights of data principals. There is a requirement of effectively communicating information related to various factors, such as the nature, manner and purpose of processing, etc. to the data principals. The obligation of transparency has a close nexus with fairness and trust. While precautionary (such as the obligations of fair and reasonable processing, [73] purpose limitation,[74] and collection limitation,[75] etc. which the Bill, 2019 had proposed to adopt) and remedial measures for transparency and accountability are intended to protect informational privacy rights of the data principals, the data protection regulator has the primary responsibility for enforcing these measures.

In order to not let the compliances burden the data fiduciaries, relaxing the requirements is counterproductive to informational privacy protection, instead the regulator may device various approaches to encourage and facilitate the compliances. The same may also help the data protection

---

[71] Matthew Rosenberg, et. al., *How Trump Consultants Exploited the Facebook Data of Millions,* THE NEW YORK TIMES, (March 17, 2018) available at https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-camlpaign.html, (last visited on Aug. 19, 2022).

[72] Julia Carrie Wong, *Uber concealed massive hack that exposed data of 57m users and drivers*, THE GUARDIAN, (November 22, 2017) available at https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack, (last visited on Aug. 19, 2022).

[73] *Supra* note 9 at cls. 4 and 5(a).

[74] *Supra* note 9 at cl. 5.

[75] *Supra* note 9 at cl. 6.

regulator to address the concerns of maintaining healthy competition in the market. Compliances for ensuring informational privacy protection, it is presumed, hinder research and development in technology, however, even if there is merit in this argument, not mandating compliances will have the effect of disregarding privacy. The use and deployment of privacy sandboxes under the supervision and monitoring of the expert data protection regulator is a privacy sensitive solution to the problem.

In addition to the independence guaranteed by law, the most important factor for the Data Protection Authority (DPA) to perform its role effectively is the DPA's ability to cooperate and seek continued cooperation with all other regulators in India . The Bill, 2019 had advocated for sector agnostic-approach to data protection, independent regulators for different sectors will have to co-operate with the Data Protection Authority to uphold rights to informational privacy. The independent regulators such as the Reserve Bank of India, the Competition Commission of India, the Securities Exchange Board of India, the Telecom Regulatory Authority of India, etc. are required to co-operate with the Data Protection Authority of India in their functioning. To resolve the conflict between intellectual property protection and data protection, the regulator will have to consult the respective statutory authorities created for different intellectual property forms in India. Thus, seeking and securing the co-operation of these expert bodies along with multi-stakeholder consultations are the ways to ensure proper balancing between the conflicting interest at the intersection.

5. Conclusion

The domains of protection of intellectual property rights and informational privacy rights intersect with each other

especially in the case of copyright protection of databases, protection of trade secrets and patents for emerging technologies. Many challenges are posed by this intersection especially to the right to access and conformation and right to data portability of the data principals. The two protections emerge as competing and conflicting with each other. Recognising the social value in privacy, understanding the nature of data and being responsive to it by conceptualising the role of data protection regulator as an entity focused on balancing the conflicting interests and securing co-operation with various sectoral regulators is the best way forward.