Journal of Intellectual Property Studies
Vol. 2 (02), July 2019, pp. 54-62

DATA RIGHTS 2.0: SHIFTING SANDS OF USAGE RIGHTS IN USER-DATA

ABHINAV SHRIVASTAVA*

With the recognition of a right to privacy as a fundamental right, and the proposed introduction of a data protection regime recognizes the user's right and interest to retain control over the processing of his/her information, the technology industry is placed at an inflexion point.

This article examines current practice with user-information and profile databases and the manner in which current law has facilitated the growth of opaque analytical and profiling practices and thereafter considers the likely impact that the proposed data protection regime would have on current aggregation and profiling practices with user-data.

The article also considers current value-models for technology enterprises, which are premised on user-data aggregation and assertions of database ownership, and projects the likely changes to such modelling that would be occasioned by the implementation of the proposed data protection regime.

* Abhinav Shrivastava is a Counsel at LawNK, a boutique Sports, Media and Technology law firm based in Bangalore.

I. INTRODUCTION

Technology enterprises have long derived their enterprise value through their accumulation of user data and profiles – to the extent of user data being the principal strategic asset for pure tech/online enterprises such as Google and Facebook.[1]

With user data driving value, business models and business processes within the ecosystem itself are geared towards acquiring users and accumulating data-banks of user-profiles with information ranging from names and contact information to browsing histories and spending patterns,[2] and with the advent of 'Big Data' analytical models, even mundane matters such as routines and habits.[3]

For example, purchases of milk through an online supermarket can be tracked to create a model for household consumption and drive suggestions and advertisements for milk at the opportune time as determined by the model. With the available storage and processing capacity levels, this can be replicated across product purchases and user-accounts.

With the increasing pervasiveness of mobile telephony and wearables, even unit level experiential user data such as moods, interactions and physical/intellectual activities,[4] is capable of collection and profiling. For example, with real-time geo-positioning data tracking, having similar travel patterns or having two devices in close proximity for an extended period, may cue a social media platform to suggest introducing the profiles associated with each device into their respective networks.

A favourable ecosystem with limited legal impediments and oversight has allowed for greater expansion of both the quantum and the quality of user-data undergoing collection and processing, and facilitated assertions of ownership by the data processor based on notions of authorship and reduction to a tangible form under intellectual

[1] Pauline Glikman and Nicolas Glady, *What's The Value of Your Data*, TECH CRUNCH, Oct. 13, 2015, (last visited Nov. 21, 2018), https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/.

[2] Nikhil Agarwal, *How Amazon, Flipkart use data analytics to predict what you are going to buy*, LIVEMINT, Nov. 16, 2018, (last visited Nov, 21, 2018), https://www.livemint.com/Companies/RX5eOy12n5JFJu617G5GnM/Amazon-Flipkart-data-analytics-ecommerce.html.

[3] Sarah Pink, et al., *Mundane data: The routines, contingencies and accomplishments of digital living*, BIG DATA & SOCIETY, (January-June, 2017), (last visited Nov. 21, 2018), https://journals.sagepub.com/doi/10.1177/2053951717700924.

[4] Clause Castelluccia, *Behavioural Tracking on the Internet: A Technical Perspective* in EUROPEAN DATA PROTECTION: IN GOOD HEALTH? 21, 23 (2012).

property laws. However, such practices stand to conflict with the user-centric approach and grant of greater autonomy and determinative rights to an individual user in relation to his/her personal information proposed by the new privacy and data protection regulatory paradigm.[5]

This article seeks to examine this potential scenario and address the question of how the current intellectual property regime would be reconciled with the emerging framework of privacy and informational self-determination in the matter of user-data.

II. USER-DATA RIGHTS IN THE CURRENT LEGAL FRAMEWORK

The intellectual property rights framework has long recognised propriety rights in databases within the scheme of copyright, particularly in the case of customer-lists.[6] Even with the shifting of the Indian legal position on copyrightable content from 'time and effort' to 'exercise of skill and judgement' as the determinative standard,[7] as the expectation of judgement to qualify for copyrightability has been kept to a 'minimal level of creativity,[8] databases continue to be copyrightable if their compilation involves some amount of intellectual effort evident in the manner of selection, co-ordination and arrangement of underlying data.[9]

As copyright is designed to determine and assign ownership in creations and work products,[10] such recognition attributes ownership and title in the database or compilation to the entity that creates the database, either by collating the information itself or commissioning its compilation, i.e., the data-controller.

In the case of user-databases, with the range of behavioural and interactional information undergoing collection across multiple touch-points, the act of processing and reducing this information into a user-profile requires the expending of intellectual effort in selecting information for inclusion and rendering the raw-data into a form that

[5] See Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1; REPORT OF THE COMMITTEE OF EXPERTS CHAIRED BY JUSTICE B.N SRIKRISHNA, A FREE AND FAIR DIGITAL ECONOMY – PROTECTING PRIVACY, EMPOWERING INDIANS, (last visited November 28, 2018) http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.

[6] See Burlington Home Shopping v Rajnish Chibber, 61 (1995) DLT 6.

[7] Eastern Book Company v. D.B. Modak, (2008) 1 SCC 1, ¶ 37,38.

[8] *Id. at* ¶ 34.

[9] *Id. at* ¶ 38.

[10] Section 17, The Copyright Act, No. 14, Acts of Parliament, 1957.

suits the analytical purposes and ends of the data-controller. In this manner, the act of processing the data serves to satisfy the minimum level of creativity expected for copyrightability and serves to support claims of copyright in the user-database.

Also, the collection of behavioural information itself involves the observation of user conduct and its reduction into machine-readable form, where reduction itself involves analysing and drawing inferences from the conduct to create a record that is distinguishable from the underlying observed behaviour. Thus, the record itself stands to be copyrightable with ownership attributed to the creator (i.e. the data-controller) of the same.

In contrast to the copyright framework, the current rights framework on privacy and data protection is fairly rudimentary and lacks clarity on the assertible rights of the data provider. A data provider's privacy rights and expectations against private (non-state) actors are currently defined by the rules prescribed under the Information Technology Act, 2000 ("IT Act").[11] These rules are contextually placed within liability safe-harbours provided under the IT Act to processors of sensitive personal data and intermediaries,[12] and are limited in ambit, to information of a sensitive nature concerning an individual, i.e. information such as passwords, financial information and medical records.[13]

Within these constraints, the rules seek to implement norms of consent and disclosure for the collection, use and transfer of sensitive personal information,[14] and generally an obligation to maintain a privacy policy with disclosures on the nature and purpose of collection of personal information by a user-data processor.[15] Even in this matter, the rules limit personal information to information that identifies an individual,[16] leaving behavioural information or derivative data outside of this purpose disclosure requirement.

While these norms were intended to provide procedural safeguards in the matter of the

[11] See the Information Technology (Reasonable Security Practices and Procedures And Sensitive Personal Data Or Information) Rules, 2011; The Information Technology (Intermediaries guidelines) Rules, 2011.
[12] Section 43A, 79, The Information Technology Act, No. 21, Acts of Parliament, 2000.
[13] *Id.* at Section 43A, ; Rule 3, Information Technology (Reasonable Security Practices and Procedures And Sensitive Personal Data Or Information) Rules, 2011.
[14] Rules 5-7, Information Technology (Reasonable Security Practices and Procedures And Sensitive Personal Data Or Information) Rules, 2011.
[15] Rule 4, Information Technology (Reasonable Security Practices and Procedures And Sensitive Personal Data Or Information) Rules, 2011.
[16] Rule 2(i), Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

collection, use and disclosure of personal and sensitive personal information,[17] and thereby grant greater oversight and some control to a data-provider in relation to his/her personal and sensitive personal information, in the absence of an umbrella data protection regime, these norms were reduced to the practice of drafting wide purpose declarations and obtaining widely framed user consents for current and potential uses.[18]

The cumulative effect of having a mature and defined copyright framework with ownership attribution to the data-controller, and a rudimentary consent-and-disclosure mandate that is limited to sensitive personal information, is that data-controllers are effectively able to collect and aggregate personal data to create user profile databases independent of user-preference or expectation of privacy, and engage in unrestricted unit-level and mingled user-data processing and analytics for insight and derivative data generation.

III. EVOLVING PRIVACY NORMS AND THEIR IMPACT ON THE CURRENT LEGAL FRAMEWORK

The right of privacy has historically been an under-served right within Indian jurisprudence, with it recognition limited to a right against intrusive or excessive surveillance by State agencies,[19] and a right to seek damages for unjustified invasions of one's private space.[20] These pronouncements have symptomatically addressed intrusions into a person's expected private sphere, but avoided the subject to the ambit of the private sphere and the actionable rights exercisable by a person in relation to his/her person and personal information.

This matter was finally addressed by the Supreme Court in the case of Justice K.S. Puttaswamy (Retd.) v. the Union of India,[21] where the Court definitely found the right to privacy to be fundamental right under Article 21 (Right to Life) of the Constitution.[22]

---

[17] Ministry of Communications, *Impact of Privacy Policy Changes by Google*, (Mar. 30, 2012), (last visited on Nov. 29, 2018), http://www.pib.nic.in/newsite/erelcontent.aspx?relid=81971.

[18] Rahul Mattan, *India's privacy non-law*, LIVEMINT, Dec. 07, 2016, (last visited on Nov. 29, 2018) https://www.livemint.com/Opinion/C4NOYNosPTZuRGjgH7UMLP/Indias-privacy-nonlaw.html.

[19] Karak Singh v State of Uttar Pradesh, 1964 SCR (1) 332, 335-6; People's Union of Civil Liberties v Union of India, (1997) 1 SCC 301, 307.

[20] R. Rajagopal v. State of Tamil Nadu, AIR 1995 SC 264, ¶ 9; Kushwant Singh v. Maneka Gandhi, AIR 2002 Delhi 68, ¶ 26-28.

[21] Justice K.S. Puttaswamy (Retd.) v. the Union of India, WP Civil No. 494 of 2012.

[22] *Id.* at 262.

The Court defined the right of privacy as the reservation of a private space for the individual comprising of those intimate matters over which the individual has an expectation of privacy,[23] these intimate matters have been worded in terms of aspects of personality such as thoughts, beliefs, preferences and behavioural patterns which are personal to the individual.[24]

In the context of the informational age, with its ability to track and aggregate user conduct to create user-profiles that detail interests, habits and preferences, the Court also recognised an individual's right and interest in protecting his/her identity,[25] and thereby determine access and use of his/her personal information. Proceeding from such recognition, the Court also directed the State to put in place a robust legal regime and framework designed to secure an individual's right of privacy and informational determination,[26] with due regard to the: (i) centrality of consent and (ii) non-discriminatory data processing.[27]

In line with the Supreme Court's direction, both the State appointed Committee of Experts chaired by Justice B.N Srikrishna and the Telecom Regulatory Authority of India presented their reports and recommendations on the core principles and proposed structure of a Data Protection Regime in India.[28] The Report of the Committee of Experts ("CoE Report") is wider in scope and provides recommendations and a draft bill for a Data Protection statute applicable across industries, while the Telecom Regulatory Authority of India's Recommendations ("TRAI Recommendations") seek to provide telecom sector-specific recommendations to secure a user's privacy expectation.

The CoE Report fundamentally recasts the relationship between the data provider and the data collector by rendering the data-provider as a data principal and the data-controller as the data-fiduciary in relation to the provider's personal information.[29] In essence, this reorders the role of the data-controller from an entity in control of the personal information to an entity that holds the information in trust for the data

[23] *Id.* at 263.
[24] *Id. at* 242-43.
[25] *Id. at* 252.
[26] *Id. at* 252-254.
[27] *Id. at* 252.
[28] COMMITTEE OF EXPERTS, *supra* note 5; Telecom Regulatory Authority of India, *Recommendations on Privacy, Security and Ownership of Data in the Telecom Sector*, Jul. 16, 2018, (last visited on Nov. 30, 2018) https://www.trai.gov.in/sites/default/files/RecommendationDataPrivacy16072018_0.pdf.
[29] COMMITTEE OF EXPERTS, *supra* note 5 at 7,8.

provider, and impliedly attributes to the data provider the right to determine the manner in which his/her personal information may be held and processed. The use of principal-fiduciary in referring to the relationship also attributes a duty of care,[30] and probity of a higher degree than an ordinary contractual relationship.

With respect to the ambit of 'personal information', the CoE Report places identifiability as the determinative means of categorisation, with any information that serves to identify an individual, either by itself or in association with other information, comprising of such person's 'personal information.[31] Thus, alongside the name of the individual, information such as his/her contact information, registration and identification numbers, online avatar name(s), profile code (whether internally employed or publicly assigned) and records containing personal information (like birth certificate, mark-sheets and educational qualification certificates) would also qualify, as they can be employed to trace the identity of the individual.

Proceeding from the paradigm of the data-provider being the data-principal in relation to his/her personal information, the CoE Report proceeds to place consent as the primary means of undertaking the collection and processing of personal information, with the added qualification of it being free and informed, specific to the purpose and capable of being withdrawn.[32] The CoE Report also vests the data-provider with continuing rights in the manner of processing of his/her personal information, including the right to withdraw consent or any specific part of the consent granted for processing of personal information.[33]

Alongside affirmative user rights, the CoE Report recommends purpose limited processing and data-minimisation,[34] norms of fair and transparent processing in relation to personal information,[35] and mandates the ceasing of processing on withdrawal of consent,[36] by data- processors. The CoE Report also stresses on

[30] *Id.* at 8.
[31] *Id.* at 27, 28.
[32] *Id.*
[33] *Id*, at 36, 37.
[34] 'Purpose limited processing' mandates that any processing of personal information be limited to activities and purposes for which the user has granted consent and purposes allied to the same, and any further processing be undertaking only with additional consent for such purpose; 'Data-minimisation' is the principle that the collection of personal data be limited only such information that is strictly necessary to achieve the purpose for which consent is granted, and no extraneous information be collected under such consent.'; *Id.* at 52, 53.
[35] *Id.* at 51, 52, 58, 59.
[36] *Id.* at 36, 37, 42.

anonymisation and irreversible de-identification of data to continue processing and analytical modelling after the completion of the consented purposes or withdrawal of user-consent.[37]

While the CoE Report reorders the relationship between the data-provider and data-collector/processor and prescribes usage-controls and limitations on data-processors, it leaves the question of ownership of the record open and unaddressed. The TRAI Recommendations, while building on the Committee of Experts' thoughts and recommendations on the subject, espouse similar principles on purpose limited and consent-based processing and anonymisation of data,[38] but more importantly, they also attribute the ownership of personal data to the data-provider with the data-controller rendered as custodian of data without any primary proprietary rights over personal data.[39]

The CoE Report and TRAI Recommendations emerged out of extensive consultation and provide substance to the right of privacy recognised by the Supreme Court. They represent the likely formulation of a privacy and data protection regime for India. As these recommendations strike at the fundamental relationship between a data processor and data- provider, their implementation will materially impact the conventional practice amongst data- controllers.

IV. CONCLUSION: IMPACT OF THE PROPOSED DATA PROTECTION REGIME

The intellectual property rights regime is concerned with determining ownership, with usage rights flowing from such ownership. However, the proposed data protection regime is designed to apply usage limitations housed in the consent framework, immaterial of ownership over the underlying record.

While current practice on user-data aggregation and processing has flourished within the rudimentary data protection regime prescribed by law and the favourable and mature intellectual property framework, this stands to materially change with the introduction of a user-centric and user-consent driven data protection regime as an

[37] 'Anonymisation' and 'irreversible de-identification' are practices where records containing non-personal information like purchase history and 'likes'/preferences data are de-linked from the underlying individual by irretrievably expunging any personal information or information that allows for linkage with a person from such record.'; *Id*. at 56, 57.

[38] Telecom Regulatory Authority of India *supra* note 28 at14,15, 25, 30-34.

[39] *Id.* at 15.

intermediate layer between the record and its processing.

The addition of purpose-limited data processing and reordering of the relationship of the data provider and data controller along the lines of a principal-fiduciary relationship also strike at the practice of wide-ranging data collection and aggregation and make the data-controller responsible for disclosing the purpose of collection of each data-stream and remaining transparent about these purposes.

While the CoE Report has stayed away from determining ownership, the TRAI Recommendations have specifically sought to attribute non-transferrable and non-assignable ownership, in the record of personal information to the data-provider. Such attribution of ownership with the user-data provider would effectively override current convention and lead to a delineation of ownership rights in the profile record, i.e. with personal data ownership resting with the data-provider and any non-personal profile data resting with the data- processor. For example, taking the example of milk purchase record analytics used on the first page of this article, the delineation of ownership rights in the user profile record would leave the data-processor as the owner of analytical profile generated from milk purchase transactions and the data-provider as the owner of the name and identifying information contained in the user profile.

The cumulative effect of the proposed usage and processing constraints on user-data will be a recasting of the attributable value of a user-database and a fundamental shift in the value attribution of enterprises that rely on user-data, such as technology enterprises and advertisers.

With the introduction of norms on consent-based processing and purpose-limited usage, the presence of continuing engagement with a user will remain key to retaining the right to process user data and understand the user better – making (daily) active user engagement a more relevant and legally tenable value driver than user-data aggregation and the building of profile databases. In the scheme of interlaced ownership and usage rights, it would render the retention of processing rights stemming from user consent and engagement as having greater value and utility than assertions of copyright over records of user-profiles and user-data.