

**THE HYBRIDISATION OF PROPERTY, LIABILITY AND INALIENABILITY IN DATA  
PROTECTION**

LALIT PANDA\*

*ABSTRACT*

*Notions that individuals self-evidently have or that they should be granted property rights in their personal data have been in the air since the concept first came to be linked with ideas of control and freedom as opposed to simply protection from interference. However, the idea of propertised personal data comes with various complications that stem from the commodification of facts as well the lack of acknowledgement to the source of privacy in inalienable entitlements linked to inviolate personality. In critically analysing the case for property rights in personal data, this article inquires into alternative categories within which the data protection rights can be placed, focusing particularly on Calabresi and Melamed's seminal three-way distinction between property, liability and inalienability originally proposed using transaction cost analysis. The article considers some relevant developments regarding this categorisation as well as criticism of the market paradigm it engenders, before turning to the question of personal data. Here, several considerations both, for and against propertisation are recounted, including concerns regarding government control, solutions through technological intermediation, and the manner in which individual control can prevent knowledge production through the aggregation of useful datasets. Some additional arguments against propertisation related to indeterminacy, information asymmetry and inalienability are also forwarded. Using these normative and descriptive findings, the rules of modern data protection law (based on the European consensus) are examined to assess the forms of entitlements employed. The analysis suggests that the urge to resort to easy and absolute categorisations should be actively avoided and that data protection rules should be treated as a hybrid, sui generis category combining aspects of property, liability and inalienability simultaneously.*

---

\* Lalit Panda, Research Fellow, Vidhi Centre for Legal Policy.

## I. INTRODUCTION: HOW “PERSONAL” IS “PERSONAL DATA”?

The discourse around privacy law has had a long and storied tradition of flirting with the conception of personal data as the property of the person to whom it pertains (“identified person”).<sup>1</sup> The notion has many attractions, with the foremost reason being the desire to create social acceptability regarding a person’s legal rights in their personal data. In India, the debate has gained prominence quite late in the day. In 2018, the Justice Srikrishna Committee of Experts on a Data Protection Framework for India released a draft Personal Data Protection Bill (“Srikrishna Draft Bill”) that characterised the relationship between an identified person and the entities processing their personal data as a “fiduciary” one.<sup>2</sup> Criticism emerged that the draft law had not made clear who “owned” the data and argued that clarifying this point was essential to setting the terms to any further debate on the subject.<sup>3</sup> Nonetheless, the formulation and lack of clarification on the ownership continues in the Personal Data Protection Bill, 2019, tabled in Parliament (“2019 Bill”).<sup>4</sup> The debate as to whether “property” is an appropriate way of describing a person’s rights in their personal data is important: while it is easy to simply dismiss the question as one of semantics or rhetoric, a number of important outcomes hinge on the question. One issue certainly does revolve around notions of rhetoric and the persuasion of public opinion. This has to do with the esteem granted to “property” in popular imagination as a concept that suggests a great degree of control on the part of the identified person.<sup>5</sup> The issue runs deeper, however, into detailed notions regarding how exactly the law is supposed to deal with personal data and how it is to structure legal protections granted to the identified person. Some of the oldest arguments in favour of legal recognition of informational privacy rooted the idea in “inviolable personality” and explicitly called for the recognition of new protections due to

---

<sup>1</sup> “There is some difference in legal terminology in references to this “person”. Particularly, a choice between the terms “data subject” and “data fiduciary” can be considered to presuppose answers to the questions that this article seeks to pursue. As a result, the term “identified person” shall be used and it is hoped that this also lends itself to accessibility on the part of readers.”

<sup>2</sup> Ministry of Electronics & Information Technology, *Draft Personal Data Protection Bill, 2018*, [https://www.meity.gov.in/write/readdata/files/Personal\\_Data\\_Protection\\_Bill,2018.pdf](https://www.meity.gov.in/write/readdata/files/Personal_Data_Protection_Bill,2018.pdf)

<sup>3</sup> Rajeev Dubey, *Srikrishna report: Too weak, too lenient and devoid of new ideas; accept TRAI report on data protection*, BUSINESS TODAY, July 29, 2018, <https://www.businessstoday.in/opinion/business-wise/srikrishna-report-data-protection-law-trai-recommendations/story/280757.html>; The Wire Analysis, *The Good, Bad and Ugly on India's Template for How Your Data Will be Protected*, THE WIRE, July 28, 2018, <https://thewire.in/tech/india-template-data-protection-draft-bill>; see also, Arghya Sengupta, *Why the Srikrishna Committee Rejected Ownership of Data in Favour of Fiduciary Duty*, THE WIRE, Aug 2, 2018 <https://thewire.in/tech/why-the-srikrishna-committee-rejected-ownership-of-data-in-favour-of-fiduciary-duty>.

<sup>4</sup> Personal Data Protection Bill, Bill No. 373 of 2019, [http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced-/373\\_2019\\_LS\\_Eng.pdf](http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced-/373_2019_LS_Eng.pdf).

<sup>5</sup> Lawrence Lessig, *Privacy as Property* 69(1) SOC. RES.: AN INT’L Q. OF SOC. SCI. 247, (2002); LAWRENCE LESSIG ET AL., CODE AND OTHER LAWS OF CYBERSPACE, VERSION 2.0 229, (2nd ed., 2006).

the inadequacy of physical property regimes.<sup>6</sup> Other initial and equally seminal proposals have been clear that the matter should be made one of property.<sup>7</sup> No doubt, the debate regarding how to structure the regulation of personal data must answer questions regarding whether the identified individual is simply to be protected by the state or is to actually have some measure of control over the said data so that they can also act to protect themselves and enjoy the fruits of such control.

On the other hand, this raises many concerns regarding whether this would “commodify” personal data and make it entirely open to trade in markets. In the current structure of the digital economy, the prevalence of free digital content and services means that unregulated personal data is widely used as a form of payment for such content and services. This has led, in Europe at least, to proposals regarding the treatment of personal data as “counter-performance”<sup>8</sup> and debate regarding the appropriateness of this allowance.<sup>9</sup> The status of personal data as property could also create complications in relation to the basis for determining the constitutionality of data protection’s speech restrictions. Intellectual property protections certainly seem to ward off scrutiny for potentially violating the right to free speech and expression by differentiating ideas from expressions. How would this be reconciled when it comes to the apparent status of personal data as “facts”?<sup>10</sup>

This article takes some modest steps to bring order to an already muddled debate. To facilitate this, the section that immediately follows provides some conceptual clarity on the appropriate means by which to categorise different kinds of legal entitlements and how “property” features within this framework. The third section then considers the argument in favour of propertising personal data as well as some of the criticisms levelled against this idea. The fourth section then proceeds to analyse the appropriate classification of the different rules within the model of modern data protection law that has seen the most consensus. It argues that the system should

---

<sup>6</sup> Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4(5) HARV. L. REV. 193, 195, 198-99, 205 (1890).

<sup>7</sup> ALAN F. WESTIN, *PRIVACY AND FREEDOM*, 324 (Atheneum Press, 1967).

<sup>8</sup> Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, COM(2015) 634 final, 2015/0287 (COD).

<sup>9</sup> Alex Metzger, *Data as Counter-Performance: What Rights and Duties do Parties Have?* 8(1) J. INTELL. PROP., INFO. TECH. AND E-COMM. L., 2- 8 (2017); European Data Protection Supervisor, *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, Mar. 14, 2017 “(the proposal was given effect in modified form as Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services).

<sup>10</sup> Richard H. Jones, *The Myth of the Idea/Expression Dichotomy in Copyright Law*, 10(3) PACE L. REV. 551 (1990); Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You*, 52 STAN. L. REV. 1049, (2000); Eugene Volokh, *Freedom of Speech and Intellectual Property: Some Thoughts After ‘Eldred, 44 Liquormart, and Bartnick’*, 40(3) HOUS. L. REV. 697, (2003); Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1158-59 (2005).

appropriately be treated as a *sui generis* hybrid of previously mentioned categorisations and that this is as it should be. The final section concludes.

## II. PROPERTY, LIABILITY AND INALIENABILITY: A CONFUSION OF CATEGORIES

### A. Legal Notions of Property

Many legal categories and concepts are notoriously slippery. This has indeed been true of the concept of “privacy”.<sup>11</sup> We are concerned here only with informational privacy, of course, and while that may reduce some of the indeterminacy in the meaning of the subject, it certainly does not answer the key question animating the present inquiry: does one appropriately regulate for informational privacy by creating property rights in personal data? At its core, this question is more normative than descriptive. It does not presume the existence of some rules, which it then seeks to fit into particular legal categories, but instead seeks to find the right categories and then develop rules in their mould. To this end, an initial conceptual question must nonetheless be answered: what is property and what are the rival categories to “property” from which we must choose?

*Black’s Law Dictionary* defines the term to mean “the right to possess, use, and enjoy a determinate thing (either a tract of land or a chattel)” or “any external thing over which the rights of possession, use, and enjoyment are exercised,”<sup>12</sup> thus referring to the term as both the right as well as the thing to which the right pertains. It also quotes an illuminating passage from Salmond:<sup>13</sup>

“In its widest sense, property includes all a person’s legal rights, of whatever description. A man's property is all that is his in law. This usage, however, is obsolete at the present day, though it is common enough in the older books. In a second and narrower sense, property includes not all a person's rights, but only his proprietary as opposed to his personal rights. The former constitutes his estate or property, while the latter constitute his status or personal condition. In this sense a man's land, chattels, shares, and the debts due to him are his property; but not his life or liberty or reputation. In a third application, which is that adopted [here], the term includes not even all proprietary rights, but only those which are both proprietary and in rem. The law of property is the law of proprietary rights in rem, the law of proprietary

---

<sup>11</sup> Daniel J. Solove, *Conceptualizing Privacy*, 90(4) CALIF. L. REV. 1087,1088 (2002).

<sup>12</sup> *Property*, BLACK’S LAW DICTIONARY 1335-36 (Bryan A. Garner ed., 9<sup>th</sup> ed., 2009).

<sup>13</sup> JOHN SALMOND, JURISPRUDENCE 423-24 (Glanville L. Williams ed., 10<sup>th</sup> ed. 1947).

rights in personam being distinguished from it as the law of obligations. According to this usage a freehold or leasehold estate in land, or a patent or copyright, is property; but a debt or the benefit of a contract is not.”

Readers may mark, especially, the distinctions between property rights, contractual rights, and rights that Salmond refers to as “personal rights” related to “status or personal condition”.

A three-judge bench of the Supreme Court of India, in *Vikas Sales Corporation*, considered the meaning of “property” in detail in having to determine whether the concept covered such intangible assets as replenishment licenses and exim scrips under the then prevailing export-import policy. The bench quoted a definition from an older edition of *Black’s Law Dictionary* as defining “property” to be a concept that extends:<sup>14</sup>

“...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 everyone 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....”

It should be noted, however, that even with these definitions regarding the bundle of rights usually included within the term “property”, the Court nonetheless particularly fixed upon a specific characteristic in one of the definitions it surveyed: the notion that “property” signified “things and rights considered as having a money value, especially with reference to transfer or succession”.<sup>15</sup> Finally, in determining that the relevant licenses were “property”, the Court reasoned:<sup>16</sup>

“The above provisions do establish that R.E.P. licenses have their own value. They are bought and sold as such. The original licence or the purchaser is not bound to import the goods permissible thereunder. He can simply sell it to another and that another to yet another person. In other words, these licenses/Exim Scrips have an inherent value of their own and are traded as such.”

Without further comment here, the attention of readers may only be drawn to the fact that, in this particular instance of judicial reasoning, two characteristics of a thing were treated as determinative of its being “property”: monetary value and tradability. This will prove of interest

---

<sup>14</sup> *Vikas Sales Corporation v. Commissioner of Commercial Taxes*, (1996) 4 SCC 433, at para. 23.

<sup>15</sup> *Id.* at para. 25-26 - quoting JOWITT’S DICTIONARY OF ENGLISH LAW, VOLUME-I (Sweet & Maxwell Ltd., 1977).

<sup>16</sup> *Id.*, at para. 33.

in the analysis that follows.

### **B. Property, Liability and Inalienability**

In our attempt to arrive at the appropriate classification of rights related to personal data, a particularly useful tool may be found in the sheer explanatory power of the categorisation of entitlements developed by Calabresi and Melamed. In their seminal 1972 *Harvard Law Review* article, they consider how legal systems set legal entitlements between parties with conflicting interests and when they chose to set property rules, liability rules and inalienability regimes.<sup>17</sup> They describe “property” rules as rules in which the legal system assigns an initial entitlement in favour of a particular person and then allows for the removal of that entitlement only through a transaction to which the property’s owner must consent. Crucially, the value that must be paid to remove the entitlement from the initial owner is something that is entirely within the choice of said owner. On the other hand, when it comes to “liability” rules, the legal system goes a step further: it not only assigns the entitlement to a particular person but, by setting out the extent of liability of any infringer of the entitlement, it also objectively determines how much needs to be paid by the person who is removing or destroying that entitlement. Here, the legal rule represents a collective determination regarding the value of the entitlement rather than allowing for the dominance of the subjective evaluation of the owner. Finally, they consider an entitlement to be “inalienable” when the legal system prohibits transfers even between perfectly willing buyers and sellers. Inalienability regimes determine who has the entitlement and the compensation that needs to be paid if the entitlement is damaged or destroyed, but beyond this, it also limits the entitlement itself by not considering the ability to transfer the entitlement as part of the entitlement.<sup>18</sup>

Calabresi and Melamed’s categorisation was animated by the confusion created by prevailing legal categorisations, such as the treatment of certain kinds of rights against nuisance as property rights. It should be apparent that where the law does not allow for a court injunction preventing someone from causing nuisance but instead allows only for compensation, the entitlement involved is not so much a property right as it is a liability rule: it allows for the owner’s enjoyment of her property to be curtailed by the creator of nuisance for a legally determined cost instead of a price determined by the owner herself.<sup>19</sup> But isn’t society better off if an initial owner only gives up their entitlement when they are paid their price by a buyer who values it more?

---

<sup>17</sup> Guido Calabresi and A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85(6) HARV. L. REV. 1089 (1972).

<sup>18</sup> *Id.*, at 1092-93.

<sup>19</sup> *Id.*, at 1105-06.

That way, they receive compensation as per their valuation and the person who would enjoy the entitlement (or its converse) more gets their way as well. Why should the law allow any entitlement to be destroyed without the consent of the person holding it?

Now here we come to the real normative proposition regarding choice between property and liability rules. Calabresi and Melamed use standard tools of economic analysis to argue that property rules are to be foregone in favour of liability rules where the transfer of the entitlement is valuable to society but the “transaction costs” are so high that it would be highly unlikely that any transaction ever takes place. Now, transaction costs include all the costs involved in getting a transaction to happen or the costs that may have to be borne if voluntary transactions were to be made the only way to allow for transfers. These include costs that would have to be borne by society if individuals selfishly hold out on selling their property for socially useful purposes even when offered a seemingly fair price.<sup>20</sup> To prefer a liability rule to a property rule, it isn’t necessary to establish that worthwhile transactions are impossible, only that making them happen is so costly that it’s better to set an objective, collectively-determined price in the form of liability.

This analysis also provides a succinct reason for choosing an inalienability regime: if it is too costly to pay for the damage caused by certain kinds of transactions or if the cost incurred by other persons “does not lend itself to an acceptable objective measurement”, it is best to prohibit them altogether. Selling oneself into slavery or selling one’s organs feature as examples of transactions and transfers that can come to be entirely prohibited, even when the parties immediately involved are willing to go ahead with it. It may also be stretched to refer to the invalidity of transactions when inebriated.<sup>21</sup>

### **C. Modifications and Criticisms**

The Calabresi-Melamed formulation has, over the years, given rise to a deluge of academic discussion and this may not be adequately represented here. Some contributions may be highlighted to further the analysis that comes after. One important point of departure is the emphasis placed by some scholars that the mere appearance of “transaction costs” should not be enough to switch from property to liability rules. This is particularly so because even if it may be difficult for negotiating parties to arrive at a fair resolution regarding the appropriate value of an entitlement, a judge may have even higher costs at arriving at a decision on the appropriate amount to impose as liability. This would mean that the transaction costs could easily be lower

---

<sup>20</sup> *Id.*, at 1107.

<sup>21</sup> *Id.*, at 1111-13.

than the “assessment costs” of liability-imposing courts.<sup>22</sup>

Another insight crucial for the present analysis is the view that liability rules are essentially partial property rules or ‘divided’ entitlements: while property rights protect interest in a thing absolutely, a liability rule can protect that interest partially or circumstantially while allowing for liability-based transfers when the relevant circumstances do not hold. Thus, while one may ordinarily have the absolute right to be free from bodily injury, one may lose that absolute right when someone accidentally injures us, triggering a liability rule. As Ayres and Talley argue, dividing a legal entitlement between rivalrous users can discourage them from behaving strategically (e.g. misrepresenting reservation prices during bargaining) and encourage them to bargain forthrightly:<sup>23</sup>

“Owners of divided, or “Solomonic,” entitlements must bargain more forthrightly than owners of undivided entitlements, because the entitlement division obscures the titular boundary between “buyer” and “seller.” This strategic “identity crisis” can strongly mitigate each party's incentive to misrepresent her respective valuation; each party must balance countervailing interests in shading up her valuation, as one would qua seller, and shading down her valuation, as one would qua buyer. This form of rational ambivalence, we argue, can lead the bargainers to represent their valuations more truthfully.”

This favours liability regimes as the division of entitlements created by such regimes facilitates forthright behaviour and better coordination. Similarly, some scholars have sought to rebut the argument that high ‘assessment costs’ borne by courts favour the creation of property regimes. While it might seem intuitive that the law should favour a property regime where the state cannot easily estimate ‘harm’ for the purposes of liability, this argument overlooks the fact that estimations regarding harm and regarding the cost of preventing harm would nonetheless have to be assessed at the initial stage when deciding how to assign property rights. Kaplow and Shavell point out this oversight and further argue that, liability rules tend to reveal the actual cost of preventing harm over time and that liability imposed on the basis of average estimates of harm makes for a superior rule to property.<sup>24</sup>

General criticism of the economic paradigm underlying the Calabresi-Melamed classification is

---

<sup>22</sup> James E. Krier and Stewart J. Schwab, *Property Rules and Liability Rules: The Cathedral in Another Light*, 70(2) N.Y.U. L. REV. 440 (1995).

<sup>23</sup> Ian Ayres and Eric Talley, *Solomonic Bargaining: Dividing a Legal Entitlement to Facilitate Coasean Trade*, 104 YALE L.J. 1027 (1995).

<sup>24</sup> Louis Kaplow and Steven Shavell, *Property Rules versus Liability Rules: An Economic Analysis*, 109(4) HARV. L. REV. 713, 725-730 (1996).

also of vital interest here. For instance, Schroeder argues that the classification confuses the definition of rights with the means of their enforcement.<sup>25</sup> Indeed, the paradigm does seem to focus less on the identity of the holder of the entitlement or the object of the entitlement for the holder, and fixates instead on the remedies available to prevent transfer and continue possession. One may well argue that the normative criterion of Pareto optimality is the reason for this fixation: the default understanding is that things have to be transferred to the person valuing it most for society to be better off. The pro-transfer bias appears strong enough that “damages for prior harms” are conflated with “a purchase price for involuntary sales”.<sup>26</sup> But interference with a legal right is not a *taking* or *transfer* of the legal right which may well be meant to legally vest in the original right holder.<sup>27</sup> The argument further runs that the limited and collectively-determined “price” of a liability rule does not imply that a tortfeasor has something like a “call option” on the entitlement of a tort victim. In this view, legal rules are not followed just because of the fear of punishment but because of a belief in the rule of law. There is something pernicious about suggesting that tortfeasors can “buy” the rights of tort victims just because they are only required to pay damages. Nance instead suggests that rules operate not just at the time of enforcement but at all intermediate stages where individuals look to the rules for “guidance” regarding appropriate conduct.<sup>28</sup>

A final issue with the property-liability-inalienability triad is important: this is the question of inalienability, the third and least discussed category. Schroeder argues that this category seems to fit badly with property and liability because of the bias of economic analysis towards monetisation and alienation.<sup>29</sup> But she argues that this ill fit is only because of the incorrect premise of the Calabresi-Melamed classification: the legal concepts are meant not only to clarify remedies at the time of potential transfer, but they serve to define and limit the rights as a whole.<sup>30</sup> In this conception, property and liability coexist instead of being alternates and together, they define entitlements implicitly while inalienability defines them explicitly.<sup>31</sup>

On a similar yet different note, Radin points out that Calabresi and Melamed impoverish discourse on inalienability by collapsing the different forms of inalienability related to transfer

---

<sup>25</sup> Jeanne L. Schroeder, *Three's a Crowd: A Feminist Critique of Calabresi and Melamed's One View of the Cathedral*, 84(2) CORNELL L. REV. 394 (1999).

<sup>26</sup> Jules L. Coleman & Jody Kraus, *Rethinking the Theory of Legal Rights*, 95(7) YALE L.J. 1335, 1356-64 (1986).

<sup>27</sup> Schroeder, *supra* note 25, at 429.

<sup>28</sup> Dale A. Nance, *Guidance Rules and Enforcement Rules: A Better View of the Cathedral*, 83(5) VA. L. REV. 837, 842-60 (1997).

<sup>29</sup> Schroeder, *supra* note 25, 417-20.

<sup>30</sup> Schroeder, *supra* n.25, at 436, referring to the arguments of Ayres and Talley, *supra* note 23.

<sup>31</sup> Schroeder, *supra* note.25, at 428-29.

and loss of control into a form of non-saleability (which she calls “market-inalienability”) related only to transfer through sale.<sup>32</sup> She argues persuasively that while market rhetoric can appear to come to the same conclusions that she does on the question of inalienability, there are problems with engaging in universal commodification of all things and justifying inalienability only in terms of the economic efficiency it promotes (problems, for example, with the economic argument that rape is problematic only because it is difficult to measure its cost for the victim). Thus, she argues that while universal commodification may only seem like a matter of rhetoric, it is pernicious because: (1) it would promote risky decision-making or the serious risk of error in judgment on the part of imperfect practitioners, (2) it would cause serious injury to “personhood”, for example by treating interests bodily integrity as fungible, and (3) it would change the texture of human interactions and values.<sup>33</sup>

Both the initial description of the Calabresi-Melamed classification as well as the discussion on its shortcomings will prove useful in our analysis of personal data and its appropriate characterisation. We must first consider, however, the proposal on propertisation.

### III. THE IDEA OF PROPERTISED PERSONAL DATA

#### A. The Market for Privacy

The idea of treating personal data as property emerges directly from the human interests that informational privacy seeks to satisfy. The desire for “control” over information is a popular conception of informational privacy rights. “Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.”<sup>34</sup> As discussed earlier, these conceptions of control appear facially identical to the rhetorical notion of property as a right where the owner has an absolute legal entitlement to take decisions regarding the use and disposal of the owned thing. Unsurprisingly, the turn of the millennium saw a host of proposals that personal data should be treated as property.

More modest proposals couched themselves in terms of contractual “default rules” or rules that automatically apply in contractual transactions unless specifically negotiated around at the time of setting the terms.<sup>35</sup> In an early contribution on this point, Richard Murphy rebutted the then-prevalent economic critique to find that “the skepticism in the economic literature is overstated”

---

<sup>32</sup> Margaret Jane Radin, *Market-Inalienability*, 100(8) HARV. L. REV. 1849, 1864 (1987).

<sup>33</sup> *Id.*, at 1877-87.

<sup>34</sup> WESTIN, *supra* note 7, at 7.

<sup>35</sup> Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1447 (2001).

and that while the economic vision that better access to information promotes market transactions remained true,<sup>36</sup> there were important efficiency-based reasons to protect privacy as property through default contractual rules rather than setting up default rules in favour of disclosure.<sup>37</sup> Another example of such default rules was forwarded by Pamela Samuelson, in the form of an analogy with the default rules surrounding trade secrecy:<sup>38</sup>

“Trade secrecy law facilitates transactions in information while at the same time providing default rules to govern uses and disclosures of protected information and setting minimum standards of acceptable commercial practice. Information privacy rights, like trade secrecy rights, can be based on contractual agreements, on conduct between the parties from which it is reasonable to infer that information was disclosed in confidence and use and disclosure beyond those purposes is wrongful, on the use of improper means to get the information.”

Significantly, the proposal hinges on the ability to licence out personal information to specific persons for specific uses and to prohibit uses that are not so permitted (i.e. “limited purposes”). This, as we shall see later, is a form of regulation linked more with use than with transfer rights and is the structure of more modern forms of data protection. Equally significant though is her view that trade secrecy could not be freely treated as a question of “property” given certain characteristics that relate it to “confidential understandings” and “unfair competition law”.<sup>39</sup> The problem with resorting to default rules in contract law is, of course, that the rules only bind the parties to the contract and are not applicable, as is the case with property law, to the world at large (this is the problem of “privity”).<sup>40</sup>

Vera Bergelson engages with the appropriate choice of systems more explicitly, finding that between the existing regimes of tort and property law, torts focused too much on secrecy, allowed only for negative rights preventing encroachment rather than affirmative rights allowing for control, and relied too much on case-by-case enforcement rather than the general applicability of property rights to affirmative control over all forms of information, regardless of secrecy. Her analysis also touches briefly upon the merits of a property regime based on the Calabresi-Melamed formulation. However, it relies on the idea that property systems are less

---

<sup>36</sup> See, for instance, Jerry Kang, *Information Privacy in Cyberspace Transactions* 50 STAN. L. REV. 1193, 1218 (1998), (citing George J. Stigler, *An Introduction to Privacy in Economics and Politics*, 9 J. OF LEGAL STUD. 623, 628-33 (1980)).

<sup>37</sup> Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2383-84 (1996).

<sup>38</sup> Pamela Samuelson, *Privacy as Intellectual Property?* 52(5) STAN. L. REV. 1125, 1152 (2000).

<sup>39</sup> *Id.*, at 1153-55.

<sup>40</sup> LESSIG, *supra* note 5, at 230; Solove, *Conceptualizing Privacy*, *supra* note 11, at 1113; Richards, *supra* note 10, at 1165-81.

intrusive and are to be treated as efficient generally with liability rules being the exception. Significant in the choice is her argument that it would be difficult to establish the quantum of harm beyond a very negligible amount, if enforcement of privacy were to be on the basis of tort.<sup>41</sup>

Jerry Kang provides a detailed account of the problem of informational privacy particularly in the context of digital transactions and favours propertisation by forwarding what he refers to as “the market solution”. He accepts that there cannot be any automatic presumption of property rights given that an individual and the collector of her data may have engaged in some “joint production” of the personal data database in the possession of the collector.<sup>42</sup> He also makes an important point in arguing that informational privacy may be a “public good”:<sup>43</sup>

“A public good has the qualities of non-rivalrous consumption and difficulty in excluding non-paying beneficiaries. Information often has these qualities to some extent, and personal data generated in cyberspace are no exception. Indeed, the digitalised environment promotes non-rivalrous consumption—because copies are as good as the original—and makes exclusion harder because information is collected and shared cheaply.”

At the same time, he distinguishes between the results of a difficulty in “exclusion” in cases like intellectual property and the situation with informational privacy. Ordinarily, a public good can result in a “free-rider” problem where individuals enjoy the property without paying for it if it is difficult to exclude access. The resultant underproduction may form the economic rationale for intellectual property, but it does not have the same result with privacy:<sup>44</sup>

“First, increased production of copyrightable materials may be an unmitigated good, but increased production of personal information is decidedly mixed. In particular, it threatens individual privacy. Second, the likelihood of underproduction is uncertain. Personal information is jointly produced by an individual and the information collector interacting in cyberspace. The individual does not spend any resources for the express purpose of generating personal data; instead, the data are generated as an unavoidable by-product of cyberspace activity.”

Exclusion can nonetheless be made possible by data security and contractual norms. These

---

<sup>41</sup> Vera Bergelson, *It's Personal but Is It Mine? Toward Property Rights in Personal Information* 37 UC DAVIS L. REV. 379, 414-419 (2003)

<sup>42</sup> Kang, *supra* note 36, at 1246.

<sup>43</sup> *Id.*, at footnote 237.

<sup>44</sup> *Id.*

differences with intellectual property inspire Lessig to argue that property protection should be strict when it comes to privacy:<sup>45</sup>

“Intellectual property, once created, is non-diminishable. The more people who use it, the more society benefits. The bias in intellectual property is thus, properly, towards sharing and freedom. Privacy, on the other hand, is diminishable. The more people who are given license to tread on a person’s privacy, the less that privacy exists. In this way, privacy is more like real property than it is like intellectual property. No single person’s trespass may destroy it, but each incremental trespass diminishes its value by some amount.”

Both Kang and Lessig concede at various points, that there are imperfections to a market in personal data. For Kang, privacy is subject to a number of non-market perceptions that make it a human value or a “civil or human right” that we may not “comfortably peddle away in the marketplace.”<sup>46</sup> However, he hesitates to turn to inalienability as the appropriate approach as this would risk “surrendering control over information privacy to the state.”<sup>47</sup> Like Kang, Lessig is interested in the propertisation of personal information because of the control it vests and because of the subjective valuation that it promotes, one that Lessig says is implicit in the divergence in concern towards privacy that individuals have.<sup>48</sup> Lessig also agrees that there are high transaction costs when it comes to digital transactions related to privacy: individuals do not display the ability to evaluate the risks they undertake to bear by agreeing to privacy policies and notices. While such high transaction costs may suggest a move from property rules to liability rules, Lessig differs: in keeping with his general assertion that “code” and technological infrastructure can serve the purposes of legal architecture, he argues with McGeeveran in favour of technological interventions like Programmed Privacy Promises (P3P), protocol that can serve to lower transaction costs by intermediating between the individual and the service provider, communicating privacy concerns effectively, and treating the acceptance of the resultant tailored offer as a contract.<sup>49</sup>

## **B. Problems with Personal Data Propertisation**

Critics have been equally strident regarding the problems with propertisation of personal data. A

---

<sup>45</sup> LESSIG, *supra* note 5, at 231.

<sup>46</sup> Kang, *supra* note 36, at 1266.

<sup>47</sup> *Id* at 1266-68.

<sup>48</sup> LESSIG, *supra* note 5, at 231.

<sup>49</sup> *Id* at 228-231; William McGeeveran, *Programmed Privacy Promises: P3P and Web Privacy Law*, 76(6) N.Y.U. L. REV. 1813, 1843 (2001).

key problem is the concern that unlike intellectual property, which creates property rights in fixed and tangible expressions of ideas, an extension to personal data would create a property right in facts: “The complexity of personal information is that it is both an expression of the self as well as a set of facts, a historical record of one's behaviour.”<sup>50</sup> An important consequence of property rights in personal data is that it ignores very significant questions on the utility of facts about an individual in engaging with the person at all. In a society of existing and growing interaction, solitude and control over access are certainly important, but one cannot be expected to interact with individuals if we are to know absolutely nothing about them unless they choose to let us know. This concern attains significance when it comes to the free speech implications of, say, a whistle-blower being restricted from declaring personal information for an important public purpose. But it can be important to varying degrees for *any* kind of interaction.

Neil M. Richards argues that there are important ways in which many privacy restrictions are not speech restrictions and that even where privacy restricts disclosure, the infringement may not be of “protected speech” and would in any case be subject to rational basis review that may easily be met by privacy proponents.<sup>51</sup> This would be a nuanced way of balancing privacy and free speech and would involve distinguishing between types of speech. Property rights in personal information, on the other hand, are more invasive of free speech. Diane Zimmerman notes, for example, that treating information as property tends to neutralise First Amendment arguments in the United States (as with intellectual property rights).<sup>52</sup> In the Indian context, rather than defend informational privacy against free speech criticisms through a property dynamic, it would be important to note that the right to privacy generally has been recognised as running across concepts like inviolate personality, liberty and even free speech, without any reliance on the concept of property.<sup>53</sup> As the property rubric does not form the basis of privacy, restrictions with free speech should be justified in a different manner than is done with intellectual property.

A further problem with assigning ownership to personal data, as discussed previously, emerges as a result of joint creation of the personal data itself or in the compilation of datasets that derives value from each piece of data included in it.<sup>54</sup> Similar issues emerge when we consider that the degree of control that we may seek to grant in relation with personal information can

---

<sup>50</sup> Solove, *Conceptualizing Privacy*, *supra* note 11, at 1113.

<sup>51</sup> Richards, *supra* note 10, at 1165-81.

<sup>52</sup> Diane Leenheer Zimmerman, *Information As Speech, Information As Goods: Some Thoughts on Marketplaces and the Bill of Rights*, 33(3) WM & MARY L. REV. 665, 665-72 (1992).

<sup>53</sup> Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

<sup>54</sup> Solove, *Conceptualizing Privacy*, *supra* note 11, at 1113.

vary wildly when it comes to type of information in question. For instance, a person may want to retain strict control over her health records or information regarding sexual orientation but may be perfectly at ease disclosing her professional credentials or educational status. The fact that we accord different degrees of privacy to different aspects of our lives certainly militates against any broad grant of property status to all personal information.<sup>55</sup> However, even in relation with data that is considered sensitive, propertisation appears to be counterproductive. Barbara J. Evans argues convincingly that in the case of health data rules in the United States, the existing framework is very similar to what patients would enjoy if they were explicitly protected by a property rule, and yet the grounds available to make non-consensual use of such data are so similar in varying regimes that it would suggest that property is not the right mode at all.<sup>56</sup> She instead suggests that the rules tend to take on features of “pliability rules”:<sup>57</sup>

“Pliability, or pliable, rules are contingent rules that provide an entitlement owner with property rule or liability rule protection as long as some specified condition obtains; however, once the relevant condition changes, a different rule protects the entitlement — either liability or property, as the circumstances dictate. Pliability rules, in other words, are dynamic rules, while property and liability rules are static.”

“Pliability rules” depart from the strict categories of “property” and “liability”, allowing for things to be subject to different rules when certain conditions are met. For example, a property right like a patent, ordinarily transferable only on consent, may be transformed into a liability rule involving legally determined fees when the conditions for compulsory licensing are met. What this means for Evans is that a default rule of consent-based data access rules can shift to non-consensual access under specified circumstances. This in itself is a very significant insight regarding the nature of informational privacy rules, but she further buttresses these findings with the prescription that such rules should draw upon a long tradition of “successful American infrastructure regulation”, because the question of ownership is simply a misguided one. Evans is referring here to the manner in which aggregated personal data datasets can serve as a kind of public infrastructure for the conduct of various useful activities that are made impossible without the creation of these datasets. She argues that “[a] major challenge in twenty-first century privacy law and research ethics will be to come to terms with the inherently collective nature of knowledge generation in a world where large-scale informational research is set to play a more

---

<sup>55</sup> *Id.*, at 1114.

<sup>56</sup> Barbara J. Evans, *Much Ado About Data Ownership* 25(1) HARV. J. L. AND TECH. 69, 77-86 (2011).

<sup>57</sup> Abraham Bell & Gideon Parchomovsky, *Pliability Rules*, 101(1) MICH. L. REV. 1, 5 (2002).

prominent role.”<sup>58</sup> Medical research datasets are thus of interest to the public at large. These arguments are linked with what we have already seen: that individual control over personal data can be an ill-fitting paradigm when we are confronted with the importance of some datasets and the bias and reduction in statistical accuracy of the dataset when a person refuses to participate:<sup>59</sup>

“Many important types of informational research must be done collectively with large, inclusive datasets. An individual’s wish not to participate, perhaps motivated by privacy concerns, potentially places other human beings at risk and undermines broader public interests—for example, in public health or medical discovery—in which the individual shares. Existing regulations lack tools to resolve this complex dilemma.”

Accordingly, she argues that “[t]he right question is not who owns health data but instead, the debate should be about *appropriate public uses* of private data and how best to facilitate these uses while adequately protecting individuals’ interests.”<sup>60</sup> Once again, we see that the specification of the particular “public use” or purpose is an important step to striking a balance between public and private interest.

### **C. Indeterminacy, Information Asymmetry, and Inalienability**

In addition to this array of reasons to avoid propertisation as well as ignore the question altogether, four additional reasons may be supplied:

*First*, it is worth considering the difficulties created by the indeterminacy of the status of personal data as personal. Copyright zeroes in on tangible and fixed expressions and the existence of the copyrightable material in some form lends itself to propertisation. On the other hand, the law has at best a loose hold on the fixedness of “personal data”. For data to be personal data, the person to whom it relates must be “identifiable”. For one matter, attempts at de-identification or anonymisation (the removal of personal characteristics from personal data so as to mask it or make it non-personal) can be met with a bewildering range of tools by which re-identification is made possible, reverting the status of the data back to personal data.<sup>61</sup> What is more, the best attempts at ascertaining the incidence of personal data nonetheless stress on the importance of the possibility of identification by aggregation and the consequent significance of the identity of

---

<sup>58</sup> Evans, *supra* note 56, at 76.

<sup>59</sup> *Id.*

<sup>60</sup> *Id.*, at 77.

<sup>61</sup> Jules Polonetsky et al, *Shades of Gray: Seeing the Full Spectrum of Data De-identification*, 56(3) SANTA CLARA L. REV. 593, 594 (2016), see also Paul M. Shwartz and Daniel Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L.Q. REV. 1814 (2011).

the entity processing the data. Thus, the recitals to the EU's General Data Protection Regulation ("EU GDPR") state:<sup>62</sup>

"To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments."

Thus, to determine whether some data is personal data, legal inquiry must enter into the question of how that data can be combined with other data to identify a person and in assessing this criterion, would look into "the means reasonably likely to be used" by the relevant person. Given the set of "objective factors" listed, it should also appear that what is personal data in the hands of some entity or person may not be personal data in the hands of another, simply because the latter does not have the means to effectuate the identification. This indeterminacy regarding the easily modifiable status of personal data and the dependence on circumstances means that,<sup>63</sup> while "property" rules are possible to imagine, they make for an ill fit given that the dynamic nature of their incidence can give rise to harms without knowledge and by accident.

*Second*, arguments in favour of propertisation tend to underestimate the deeply rooted information asymmetry underlying the failure in the personal data market.<sup>64</sup> To put it briefly, the two transacting parties each hold some relevant sets of information that is appropriate to the optimal transaction and allocation of rights. The identified individual, for example, has the best access to information regarding which of their aspects they would like to keep private or restrict access to and under what circumstances. This self-knowledge regarding their privacy preferences can be considerably detailed and contextual, and their willingness to represent this information in the form of broad prohibitions or permissions can, in many circumstances, simply be inaccurate classifications. For example, a general permission to use location data may fail to account for various specific situations in which that location data can come to be combined with the location data of other persons one has met or visits of a sensitive nature to particular places. A general

---

<sup>62</sup> Recital 26, European Union General Data Protection Regulation, Regulation (EU) 2016/679.

<sup>63</sup> Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data*, European Commission, June 20, 2007, art. 29.

<sup>64</sup> See George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84(3) THE Q. J. OF ECON. 488, (1970).

prohibition, on the other hand, can be too restrictive of providing access to other parties. These entities that gain access to personal data themselves have information important to the transaction: specific information regarding particular purposes of processing the data, particular parties to whom it may be transferred, particular pieces of other data with which this data may come to be combined etc. All of this is relevant to determine how the privacy of an identified individual may be affected.

The law may require disclosures, as it usually does for information asymmetries, but this runs into considerable problems: the individual would not want to disclose the specific facts about them that they deem private and is likely to cloak permissions in broad categories, while the entity processing the data may make detailed disclosures but this may be very difficult if not impossible for the individual to go through given the number of digital or information-based interactions they are undertaking and the complexity of each. This is linked to the transaction-intensive nature of informational privacy regulation<sup>65</sup> and is only likely to increase with the complexity of processing activities in the age of Big Data and algorithmic processing. In Julie Cohen's astute analysis of the risk and information-oriented regulatory responses to the growing recognition of systemic threats, she finds:<sup>66</sup>

“As societal understandings of harm have evolved to encompass more long-term and systemic effects of development, regulatory methodologies have evolved as well. The contemporary toolkit includes constructs oriented toward measuring, demonstrating, and responding to harms that are nascent and systemic, and those constructs are themselves predominantly informational. As threatened future harms have become more abstract, diffuse, and technologically complex, disputes about appropriate regulatory response have become struggles for control over the modelling and representation of systemic threats and over the burden of proof required to justify regulatory actions.”

The probabilistic and diffused nature of certain kinds of privacy harms is an important aspect of study relevant to data protection, with one scholar distinguishing “subjective” and “objective” privacy harms and even analogising them with assault and battery respectively (the former is an apprehension or threat of the latter).<sup>67</sup> These informational considerations mean that individuals have considerably reduced abilities to safeguard themselves against harm through privacy self-

---

<sup>65</sup> Suyash Rai, *Response on the White Paper of the Committee of Experts on a Data Protection Framework for India*, 3-5, [http://macrofinance.nipfp.org.in/PDF/data\\_protection\\_comments\\_suyash.pdf](http://macrofinance.nipfp.org.in/PDF/data_protection_comments_suyash.pdf).

<sup>66</sup> Julie E. Cohen, *The Regulatory State in the Information Age*, 17(2) *THEORETICAL INQUIRIES* L. 369, 389 (2016).

<sup>67</sup> M. Ryan Calo, *The Boundaries of Privacy Harm*, 86(3) *IND. L. J.* 1131, (2011).

management. This situation is considerably aggravated by the opposite of information asymmetry, in the form of transaction costs created by an abundance of information. This is caused by what is variously called “infoglut”<sup>68</sup> or informational overload and the consequent occurrence of “consent fatigue” due to which individuals find themselves with a surplus of material making it difficult for them to identify points of information relevant to their choices.<sup>69</sup> Some of these informational constraints may be possible to intermediate away through technology but one may be pessimistic that the essential asymmetry created by privacy preferences can be eliminated. In any case, one may consider the possibility of propertisation to the extent of the removal of transaction costs but make room for other legal systems to supplement it.

*Third*, a crucial distinction exists between personal data and other things that have been considered under the property rubric. This difference lies in the conceptual core of “personal data”: the idea that the person to whom the data relates should be identifiable. This criterion is essential to attain the protection of the law, and this is not accident. Data protection provides remedies to the identified or identifiable individual precisely because the person is identified or identifiable. If they were not, the kinds of harms to liberty, personhood and intimacy that informational privacy is aimed at protecting against would not be at play and protection would not be necessary. Here, the market logic comes under incredible strain: when referring to the “transferability” of personal data as property, we have had under consideration not just the initial transfers of personal data from the individual to one entity, but onward transfers to further entities and disclosures of varying degrees of publicity. While one can still conceive of some forms of consensual transfers in the instance of primary markets, when onward transfers in secondary markets become even slightly numerous, it is highly unlikely that the individual can have meaningful information and foreseeability regarding the outcomes.<sup>70</sup> In the economic view, transactions in the secondary market for personal data can be either considered to suffer from information asymmetry because of the difficulty of maintaining oversight, or perhaps it can be treated as a negative externality in which the identified individual has somehow become a third party suffering due to the market transactions of the primary parties, the buyers and sellers of her personal data. This begs the question: how is there to be any meaningful market regulation

---

<sup>68</sup> MARK ANDREJEVIC, *INFOGLUT: HOW TOO MUCH INFORMATION IS CHANGING THE WAY WE THINK AND KNOW* (Routledge, 2013).

<sup>69</sup> Daniel Solove, *Privacy Self-management and the Consent Dilemma*, 126 *HARV. L. REV.* 1880, (2013); B. W. Scherer et al, *The crisis of consent: how stronger legal protection may lead to weaker consent in data protection*, 16(2) *ETHICS AND INFO. TECH.*, 171-182 (2014).

<sup>70</sup> Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy As Property in the Electronic Wilderness*, 11(1) *BERKELEY TECH. L. J.* 1, 5-6 (1996).

without considering the individual to have an inalienable right in her personal data? This leads us to the final point.

*Fourth*, inalienability is an irreducible component of informational privacy and the grant of an inalienable right in a thing is incompatible with most conceptions of property rights. Following considerations in the EU of the problem of the exchange of digital services and content for personal data, the practice came to be permitted but the idea that personal data was somehow to be considered “counter-performance” or a “commodity” was explicitly rejected:<sup>71</sup>

“Digital content or digital services are often supplied also where the consumer does not pay a price but provides personal data to the trader. Such business models are used in different forms in a considerable part of the market. While fully recognising that the protection of personal data is a fundamental right and that therefore personal data cannot be considered as a commodity, this Directive should ensure that consumers are, in the context of such business models, entitled to contractual remedies. Union law on the protection of personal data provides for an exhaustive list of legal grounds for the lawful processing of personal data.”

Notions of informational privacy embedded into modern data privacy laws thus tend to view the right in light of its recognition as a fundamental right, as it has been in India. In advising that India follow the EU route for a strong, comprehensive legislation instead of the US sectoral/self-regulatory route to data protection regulation, Graham Greenleaf points out the significance of privacy being a fundamental right:<sup>72</sup>

“The position in India is in general principle the same as the EU: privacy is a fundamental inalienable right, with the ability of governments to derogate from it requiring considerable justification [Data protection in India] will have to meet standards approximating those of EU laws if it is to constitute the background environment within which particular legislative interferences with privacy can be justified.”

This does, of course, depend on the extent to which one sees fundamental rights like privacy being applicable in the context of the activities of private entities, either directly or in the form of a duty of the state to intervene and protect individuals from such entities.<sup>73</sup> This concern with

---

<sup>71</sup> Recital 24, Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services.

<sup>72</sup> Graham Greenleaf, *Data Protection: A Necessary Part of India's Fundamental Inalienable Right of Privacy – Submission on the White Paper of the Committee of Experts on a Data Protection Framework for India*, 4 UNSW L. RES. Paper No. 18-6 (2018).

<sup>73</sup> See Stephen Gardbaum, *The “Horizontal Effect” of Constitutional Rights*, 102(3) MICH. L. REV. 387, (2003) (For

inalienability has, however, an important corollary for the purposes of the present inquiry. It is fundamentally incompatible with property. Solove recognises the importance of maintaining inalienable rights in personal data, but for some reason suggests: “Inalienability rules do not necessarily have to limit a person’s ability to disclose or sell certain information; nor must they limit many forms of information collection.”<sup>74</sup> On the other hand, Jessica Litman is clear regarding the essential features of a property regime:<sup>75</sup>

“The *raison d’être* of property is alienability; the purpose of property laws is to prescribe the conditions for transfer. Property law gives owners control over an item and the ability to sell or license it. We deem something property in order to facilitate its transfer. If we don’t intend the item to be transferred, then we needn’t treat it as property at all. If we do intend to encourage its sale, a property model does the job admirably. Thus, we have resorted to the property model for intangible interests when we want to make it easy to sell them. Intellectual property is the paradigmatic example. The concept of alienable ownership rights in personal data is disturbing, because the opportunities to alienate are ubiquitous.”

These arguments should be persuasive that there are a number of problems with the complete propertisation of personal data. As described at length above, these problems are not just descriptive issues regarding what can be called “property” at all, but also normative issues hinging on the impact of propertisation on both economic efficiency as well as other values related to personhood. The reader would now be concerned to know that if data protection rules are not to be considered property rules, then what are they to be considered at all? Are they only liability rules? Does the regime have all the features of inalienability? A limited attempt to answer this question shall be made below.

#### IV. DATA PROTECTION AS A HYBRID SYSTEM

Presently, the European model for data protection constitutes a global model for modern data protection law, with a number of other jurisdictions emulating or altogether mirroring its framework.<sup>76</sup> India’s own steps in the form of the Srikrishna Draft Bill and the 2019 Bill also

---

studies to the “horizontal” applicability of fundamental rights); Mark Tushnet, *The issue of state action/horizontal effect in comparative constitutional law*, 1(1) INT’L J. CONST. L., 79-98 (2003); STEPHEN GARDBAUM, *Horizontal Effect*, in THE OXFORD HANDBOOK OF THE INDIAN CONSTITUTION (Oxford U. Press, 2016), at Chapter 33; Also See, *Society for Un-aided Private Schools of Rajasthan v. Union of India* (2012) 6 SCC 1, Para 126, 159 and 222.

<sup>74</sup> Solove, *Privacy and Power*, *supra* note 35, at 1455.

<sup>75</sup> Jessica Litman, *Information Privacy/Information Property*, 52 STAN. LAW. REV. 1283, 1295-96, 1299 (2000).

<sup>76</sup> Greenleaf, *supra* note 72, at 3-4, (Greenleaf refers to the adoption of the EU’s 1995 Directive, the precursor to the GDPR: “The White Paper observes ‘that there are two distinct models in the field of data protection’ (an EU model, and a US model), and that the ‘EU model appears to be the preferred mode in several countries who have

follow in the trail European experience. And this has been a considerable experience, given that about two and a half decades of enforcement history has passed since the EU's 1995 Directive on the subject was brought into force. It is this model of data protection law that the present inquiry is aimed at better understanding.

As the perceptive reader would have no doubt noted, most of the foregoing analysis has been informed by American scholarship. This literature has been surveyed and systematised above for a good reason: the analytical power of some of the tools in the interdisciplinary toolbox of this scholarship is equally effective even in making sense of the European system. Indeed, the more complex the statutory regime devised by Europe, the more useful the American toolkit can be. The interdisciplinary nature of much of the discourse, particularly the insights of economic analysis, makes particularly deep inroads especially when dealing with questions of law and policy. And this is precisely the juncture we are at: the law is ill equipped to autonomously come up with reasons for the choice between property, liability and inalienability rules. Constitutional adjudication with broad terms may reach conclusions regarding the status of an interest as a fundamental right, but it would be overambitious to consider that existing case law would somehow employ metaphoric reasoning to grasp particularly slippery concepts without the aid of existing legal rules.<sup>77</sup> One may consider how intellectual property first came to be classified as a kind of property. Faced with a similar situation, we must consider the existing legal categories but apply to them our understanding from other fields like economics and philosophy.

#### **A. The Categorisation of Rules in Data Protection Law**

A key structural feature of data protection law, and the feature of most interest to us, is a principle called “lawfulness”.<sup>78</sup> This may appear a bit redundant given that all legal rules are aimed at determining lawfulness, but the GDPR uses this terminology in a particular way. The lawfulness of processing is determined by a set of what is called “grounds” or “legal bases” that

---

adopted data protection legislations recently’. This is a considerable understatement and a misunderstanding. Over 120 countries have now enacted data privacy laws that meet or exceed the ‘1st generation’ standard of the 1980s OECD Guidelines and Council of Europe Convention 108. Of the 67 of these 120 countries outside Europe their average implementation of the ten ‘2nd Generation’ ‘European’ principles (i.e. those in the EU Directive of 1995 that go beyond the OECD Guidelines), is at least 6/10 principles. That also applies to those countries outside Europe with the highest GDP, with a privacy law. The reality, therefore, is that the current global standard of data privacy laws even outside Europe, is closer to the EU Directive than the OECD Guidelines. The US, with no general data privacy laws, is completely out of step with the rest of the world. There is one global standard – and then there is the US, increasingly isolated.”).

<sup>77</sup> See Chris Rideout, *Penumbral Thinking Revisited: Metaphor in Legal Argumentation*, 7 LEGAL COMMUNICATION & RHETORIC: JALWD 155 (2010); Steven L. Winter, *Transcendental Nonsense, Metaphoric Reasoning, and the Cognitive Stakes for Law*, 137 UNIV. OF PA. L. REV. 1105, (1989).

<sup>78</sup> Article 5, Regulation (EU) 2016/679 of The European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter, EU-General Data Protection Regulation).

an entity processing the personal data can rely on. These grounds are listed out in the GDPR in Article 6 and in India's 2019 Bill at Clause 11 and Chapter III. In both these instruments, the legality of processing is determined by providing processing entities with a multiplicity of options and, at the enforcement stage, by assessing whether the conditions in any of those options have been satisfied so as to justify the legality of the processing. The grounds run along the same lines: they include consent, the compliance with some law other than the data protection law, the performance of the function of the state or some public authority, the safeguarding of some vital interest in the event of an emergency, and a residual ground of legitimate or reasonable purposes.

The grounds for determining the lawfulness forms the backbone of these data protection instruments because these rules determine when the processing of personal data by someone other than the identified individual is legal or not. These grounds are of particular interest to us because "processing" includes mere storage or possession of personal data.<sup>79</sup> Possession of personal data is attained, in most contexts, simply by observation and thus the legality of possession presupposes the legality of the transfer of the personal data to the processing entity. One may recall that the Calabresi-Melamed model suggests that we treat a rule as a property rule if it permits subjective valuation before allowing any transfer and we treat it as a liability rule if it allows for transfer without explicit permission but imposes a collectively-determined penalty on the transferee in the form of an objective valuation of liability. Personal data seems to transfer with little friction, and it may appear that possession is the subject of analysis, but this does not prevent us from applying the model. What may immediately be noted is that the optionality created by the "grounds" system for determining legality includes within it the ability to consensually transfer and permit use of personal data as well as the permissibility of non-consensual transfer and use. Indeed, to mark the difference, Chapter III of the 2019 Bill is titled "Grounds for processing of personal data without consent".

One could thus say that because the same thing (personal data) is at the same time capable of being transferred non-consensually as well as on the basis of consent, the transfer is at least sometimes on the basis of the subjective valuation of the identified individual and her interest in personal data is at least partially protected by a property rule. Just as with a property right, the individual exercises control over the personal data and has the right to grant or refuse to grant use of the data to others. However, we are then confronted with a further issue: even after permitting the individual to transfer the right of usage of her personal data to other persons, data

---

<sup>79</sup> Article 4(2), EU-General Data Protection Regulation, and clause 3(31), 2019 Bill.

protection law does not seem to have extinguished her rights in her data. This is in evidence as a result of a number of rules. The first rule deals with the validity of consent. To allow for a transfer to be treated as consensual at all, data protection law requires that the consent be capable of being withdrawn.<sup>80</sup> The second set of rules are what are called the “data subject rights”, rights that allow the identified individual to continue to exercise some degree of control over the personal data by confirming that it is with an entity, accessing it, correcting and updating it, restricting its disclosure, erasing it, or even requiring that it be transferred to a different entity.<sup>81</sup> A third and even broader set of rules relate to the variety of entitlements that emerge across the provisions in these instruments as correlatives to the duties imposed on the entity processing the data. Broadly, these rights deal with transparency, accountability and security, but specifically they arise as entitlements because the processing entity is under related duties to carry out organisational measures, impact assessments, audits, record keeping, notifications in the event of data breaches and the setting up of grievance redressal units.<sup>82</sup>

This wide swathe of control that the individual continues to exercise in personal data that they have willingly transferred over to someone else creates some conceptual confusion. On the one hand, these statutory rights do not appear to be capable of being waived and are for all intents and purposes, inalienable. The rule requiring that consent be capable of being withdrawn, at least, pertains to the validity of consent itself and waiving that right would almost certainly be contrary to the public policy of data protection law.<sup>83</sup> However, unlike with other inalienable entitlements, the individual has been granted the ability to voluntarily transfer the *right of use* of their personal data on the basis of her subjective valuation as to the worth of the use as well as anything they may be getting in exchange. One does not ordinarily have the right to transfer things in which one has an inalienable entitlement and yet, perhaps due to the ability of data to be duplicated without diminishment, here we have a thing being transferred freely while retaining inalienable statutory interests in it.

Equally baffling is the situation with the non-consensual grounds. As mentioned above, these grounds allow for the use of personal data without consent, for example for compliance with a law, the performance of state functions, safeguarding life and limb in the event of an emergency, and a residual legitimate or reasonable purposes. Here, the individual is given no right to allow or exclude usage of their personal data because their consent is not relevant to processing on these

---

<sup>80</sup> Article 7(3) EU-General Data Protection Regulation and clause 11(2)(e), 2019 Bill.

<sup>81</sup> Chapter 3, EU-General Data Protection Regulation, and chapter V, 2019 Bill.

<sup>82</sup> Chapter 4, EU-General Data Protection Regulation, and chapter VI, 2019 Bill.

<sup>83</sup> *Murlidhar Aggarwal v. State of Uttar Pradesh*, (1974) 2 SCC 472.

grounds. On the other hand, the processing entity gains the ability to process the personal data and does not even have to pay any penalty for doing so. This means that the transfer is not on the basis of a liability rule. Does that make the right of the processing entity to use the personal data a property right? For one matter, grounds may only be invoked for what Kang would call a “functionally necessary” purpose<sup>84</sup> and what Evans would call “appropriate public uses”.<sup>85</sup> It is true that the grounds themselves constrain the potential uses to a limited set of uses that meet their criteria but the imposition of functional necessity equally emerges from the principle of “purpose limitation” which requires that personal data always be “collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes”.<sup>86</sup>

Thus, the scope of a ground and the requirement of purpose limitation both constrain the potential uses of the personal data. Limitations on the use and enjoyment of a thing may appear facially at odds with the idea of plenary control over property, but they are easily reconcilable with certain forms of property such as licenses.<sup>87</sup> What is more problematic in considering these rights to be property rights is the fact that processing entities can’t really alienate their entitlements either. Because the use implied by the non-consensual grounds is dependent on the carrying out of a “necessary” function, the question of alienation does not seem to arise as the situation of necessity cannot be transferred.

Finally, it is worth mentioning that the violation of the rules of functional necessity or any refusal to abide by the inalienable entitlements of the identified individual results in liability for the infringing entity, both in terms of compensation as well as turnover-linked penalties determined on the basis of detailed criteria that include but do not limit themselves to the immediately observable or predictable quantum of harm.<sup>88</sup> The pegging of these penalties to criteria other than harm should alleviate concerns that the assessment costs of finding the appropriate level of liability would be too high. The penalty seems to instead be linked to a form of deterrence related to the gravity of the violation through a multiplicity of linkages.

## **B. Justifying Hybridisation**

The discussion above shows that the rules under modern data protection law, personal data appears to be protected simultaneously by property, liability and inalienability rules. The

---

<sup>84</sup> Kang, *supra* note 36, at 1265.

<sup>85</sup> Evans, *supra* note 56.

<sup>86</sup> Article 5(1)(b), EU-General Data Protection Regulation.

<sup>87</sup> Samuelson, *supra* n.38.

<sup>88</sup> Clauses 57-61 and 63(4), 2019 Bill.

discussion that preceded the one immediately above also surveyed a range of reasons in favour of all three rules, but found that the classification of a thing as being protected under one regime often militated against its being considered a subject of the other regime (e.g. property is ordinarily never inalienable). The immediate task then, is to assess whether the seeming indeterminacy of the categorisation answers our initial question: whether we can talk of personal data as the property of the person to whom it relates?

The prime focus of the distinctions so far has been the Calabresi-Melamed classification. This is, however, a good point to note that their classification doesn't so much categorise things as being regulated by different kinds of rules as it categorises rules as being part of different kinds of systems. This should be apparent from the fact that they do acknowledge that entitlements can be "mixed":<sup>89</sup>

"It should be clear that most entitlements to most goods are mixed. Taney's house may be protected by a property rule in situations where Marshall wishes to purchase it, by a liability rule where the government decides to take it by eminent domain, and by a rule of inalienability in situations where Taney is drunk or incompetent."

Perhaps this pithy but previously missed insight should be the end of all our travails? Why have previous inquiries spilled so much ink on the question if we can simply say that entitlements in personal data should be "mixed"? In the context of the rules discussed immediately above, perhaps an individual's personal data is protected by a property rule where the processing entity seeks to invoke the individual's consent, by a liability rule where it seeks to use her data non-consensually and in a functionally unnecessary way, and by a rule of inalienability where it seeks to ignore the individual's withdrawal of consent or request for a right such as that of confirmation or access?

Some alternatives are worth considering, from the previous discussions regarding the appropriate usage of the Calabresi-Melamed classification:

1. *Ayres and Talley's divided entitlements*:<sup>90</sup> One could well argue that the property right has been divided up between the individual and the processing entity and that both parties now have liability rules constraining their behaviour. Neither owns the personal data but both are liable for doing things that may harm the other's recognised interests in it. The processing entity is liable if it attempts to process non-consensually and without the justification of any recognised ground of processing. The individual may have to suffer

---

<sup>89</sup> Calabresi and Melamed, *supra* note 17, at 1093.

<sup>90</sup> Ayres and Talley, *supra* note 23.

some consequence for not transferring personal data where a non-consensual ground exists for the processing entity to rely on but where the transfer depends on the individual's action. This may be some penalty for non-disclosure under some other law, but that would involve the application of a distinct rule outside data protection. Should that not be considered part of the rule system determining the status of the entitlement? The liability may be the loss of the personal data itself, but this does not seem like a liability at all as the personal data was already legally required to be transferred and was the entitlement of the processing entity. No additional liability seems to be necessarily imposed on the individual for denying personal data to the entity. Perhaps it would be appropriate to impose such liability.

2. *Schroeder's rejection of the classification*:<sup>91</sup> One could suggest that the property-liability-inalienability classification was flawed to start with and that three concepts were to be used simultaneously to define and limit entitlements without fixating on the conditions of transfer. There certainly seems to be some appeal in Schroeder's argument that the Calabresi-Melamed classification focuses more on the conditions of transfer and possession and not so much on the quality of use or enjoyment. This would, for instance, explain how the model does not seem to provide a clear answer for a regime where the primary harm that is to be regulated is created by the unspecified use of personal data for purposes that are beyond the knowledge of the identified individual. Her own ability to enjoy informational privacy as opposed to her ability to transfer or possess her personal data becomes the focus here.
3. *Litman and unadulterated inalienability*:<sup>92</sup> A focus on the traditional boundaries of the concepts as opposed to the rehashed boundaries employed by Calabresi and Melamed may lead us to argue that a thing is indeed only capable of being property if it is fully alienable and that if it is inalienable we should not refer to it as property at all. The reliance on this conception may ignore Calabresi and Melamed's interest in classifying types of rules rather than types of things but it would certainly help us answer questions on how we can translate our findings for an existing legal audience without disturbing their sensibilities.
4. *Bell and Parchomovsky's pliability rules*:<sup>93</sup> We may lastly treat the boundaries between the categories to be porous (what Bell and Parchomovsky call "dynamic" pliability rules) or

---

<sup>91</sup> Schroeder, *supra* note 25.

<sup>92</sup> Litman, *supra* note 75.

<sup>93</sup> Bell and Parchomovsky, *supra* note 57.

consider them to be overlapping (“simultaneous” pliability rules). A number of examples of such rules have been identified in the form of share ownership in mergers and acquisitions, essential facilities and antitrust damages, nuisance, copyrights, patents, the fair use doctrine, adverse possession and eminent domain. In essence, the categorisations retain their meaning but their application to things is facilitated by pointing out that the protection of a thing by one type rule can change to protection by a different rule on the basis of a trigger, whether that trigger is the passage of time or the occurrence of a particular event.

At this point, it is worth remembering the concerns that initially animated this inquiry. These concerns stemmed from the idea that referring to the right in a particular thing as a right to property could have considerable knock-on effects on how it is treated in relation with a variety of questions. A sobering realisation by the end of the analysis is that the occurrence of such knock-on effects is the result of broad categorisations of things in legal analysis as opposed to a more specific and nuanced analysis that categorises types of rules and appreciates the possibility of their co-existence. The scourge of broad categorisation and metaphoric reasoning seems so prevalent that it seems not just the playground of unstudied laypeople but also equally the preserve of legalists with fixed notions of categories. It is worth recognising that this is an inherent problem with legalistic approaches, given that legal terms and concepts are often “devoid of all semantic reference”. One may imagine that the term “ownership” has some inherent meaning of its own, but it only serves to present a number of disparate relationships under one label (e.g. one can say without referring to the concept of “ownership”, that “if you purchase something you have the right to recover it from someone who takes it”).<sup>94</sup> This is essentially so for catch-all legal terms like “property” that serves to denote “bundles” of rights, but may also denote some specific rights.

Calabresi and Melamed’s allowance for “mixed” entitlements may well refer to the different rules governing “Taney’s house” by different names, but this may not prevent legalists from finding that Taney’s relation with the house is essentially one of “property” for the purposes of more traditional legal determinations. What is true for terms like “property” can equally be true for terms like “inalienability”, tyrannically occupying the entire legal imagination on all questions of legal relations with personal data. For no reason other than to push our legal language forwards into more advanced and nuanced forms of reasoning and communication, it is appropriate that the entitlement of an individual in her personal data be referred to not as property, liability, or

---

<sup>94</sup> Alf Ross, *Tû-Tû*, 70(5) HARV. L. REV. 812, 812-825 (1957).

inalienability but as a hybrid of the three: it is a data protection right, a *sui generis* form of flexible, dynamic protection that clearly fits the description of Bell and Parchomovsky's pliability rules but with the addition of the essential elements of inalienability.

## V. CONCLUSION: RHETORIC REDUX

This article began on a note of frustration. This frustration originated in the use of legal terms like "property" loosely in the context of data protection with little regard to the potential damage this could do in the long run to the actual development of the law itself.

To assist in justifying the rejection of such propertisation, the second section analysed the seminal three-way distinction of Calabresi and Melamed between property, liability and inalienability as well as the justifications for choosing one form of legal entitlement over the other. The criterion of transaction costs was identified as a crucial consideration in the choice between the three: property rights may be foregone for liability rights if market valuations were costlier to arrive at as compared to objective, collective valuations. At the same time, variations on this premise were examined, including assertions regarding over-emphasis on the magnitude of transactions costs and under-emphasis on the utility liability rules. The section also considered criticism of the classification regarding the bias of the market paradigm in favour of transfer as well as the pernicious effects of commodification.

The third section then provided an account of the idea of propertised personal data by considering ideas related to contractual default rules, trade secrecy-like licenses, difficulties in assessing privacy harms, concerns regarding surrender of control to the state and the prospect of technological intermediation. These proposals were juxtaposed with concerns regarding the status of personal information as facts, conflict with the right to free speech, difficulties in allocation in the case of the joint production of data, the problem of degrees of privacy in types of personal data, the problems created by individual control in the aggregation of useful datasets, the insignificance of the ownership question in the face of the use question, the indeterminacy of the status of personal data as personal, intractable forms of information asymmetry, the irreducibility of the linkage between an individual and her personal data, and the incompatibility of property rights with inalienability regimes.

On the back of the descriptive and normative assertions in the previous sections, the fourth section proceeds to unpack the structure of modern data protection law as seen in the European model. After finding that the rules appear to simultaneously retain characteristics of property, liability and inalienability, the analysis arrives at the conclusion that the desire for strict categorisation is the source of the confusion and that no better antidote for this desire exists

than to promote flexibility by embracing a new category. Thus, what began as an attempt to channel discourse away from rhetoric has come to fix instead on a different kind of rhetoric. Hopefully, this journey of realisation has carried through to the experience of readers as well.