DATA WITHOUT OWNERSHIP: THE CRISIS OF IP PROTECTION IN DATA-DRIVEN ECONOMIES

Chanchal [1] & Aditya Lohani [2]

ABSTRACT

In modern digital economies, data has been a major source of value, but as the legal nature of data, there is a lack of clarity and theory. In this paper, the author focuses on the increasing lack of tie between the economic significance of data and its diminished importance in the context of conventional intellectual property regimes. By a doctrinal study of the law of copyright, patent and trade secret, the study reveals that the current IP frameworks are structurally inadequate to capture data as a legal provision that can be protected. Copyright does not protect data because it is unoriginal information, patent legislation favors technical inventions, rather than information production, and the protection of trade secrets is conditional, frail and requires secrecy. Without the provision of ownership-based protection, similar to the contribution to market concentration, regulatory issues, the de facto data property regimes in the form of contracts, platform governance, and technological controls have become established. The paper uses comparative approaches and maximising the interest of the people in arguing that uncritical data propertisation should not be one of the prior ways and governance model grounded on the notions of access, stewardship, and interoperability. It injects the conclusion that a redefinition of data governance outside the notion of ownership should take place to strike a balance between innovation, competition and societal interests.

Keywords: IPR, Data Protection, Patent, Copyright

[1] B.A.LL.B (HONS.), GLA University.
[2] B.A.LL.B (HONS.), GLA University.

INTRODUCTION

In contemporary capitalism, the foundational raw material has emerged to be the Data. It is a form of an asset or a property that possess all qualities of being created, stored, transferred, stolen or sold. It provides value, market power, and public goods to corporations, research institutions, and nations; nevertheless, the legal framework governing this resource is still disjointed and conceptually unclear. Although data is the foundation of robust economic ecosystems and new kinds of automated knowledge generation, it is difficult to integrate into the property-based frameworks that have historically supported commercial regulation and intellectual property law.

The traditional IP regimes as copyright, patent, and trade laws were created with specific normative weigh-offs between transparency and exclusivity as well as unique subject areas like technological invention, artistic expression, and confidential information. But Raw data doesn't fall into any of the categories of these law as they are neither inventions to include under patent nor expressive works in the sense of a copyright. Additionally, their protection as trade secrets frequently depends on tenuous conditions of confidentiality that are readily compromised by scale and interoperability.[3] Based on this observation, if we treat data as a property, it faces significant policy trade-offs in addition to philosophical challenges.

One jurisdictional attempt to provide particular protection for data collections is the European Database Directive and its sui generis right, however assessments reveal significant limitations in terms of breadth, efficacy, and adaptability to modern data practices. Simultaneously, platform terms of service, licensing agreements, and technological access controls function as de facto regimes of exclusion and appropriation, resulting in governance outcomes that frequently favour incumbent platforms and diminish transparency and contestability. As a result, the practical governance of data has moved primarily into private law.

These interactions create acute threats to competition, innovation, and democratic access to knowledge. Unregulated data encourages extractive practices and fragmentation of accountability; over-propertisation runs the risk of enclosing socially valuable resources and limiting research or public-interest usage; and data asymmetries generate entry hurdles and network effects that can solidify market dominance. In response, a variety of alternative governance proposals have surfaced, aiming to rebalance incentives, access, and stewardship

[3] Lothar Determann, No One Owns Data, 70 HASTINGS L.J. 1 (2018).

without merely turning data into conventional private property. These proposals range from cooperative institutions like data trusts to regulatory access frameworks and portability obligations.[4]

This article investigates the governance gap. It contends that the dilemma of "data without ownership" is both doctrinal and institutional: it stems from the mismatch between IP law and the materiality of data, as well as the emergence of private, contract and platform-driven control regimes that avoid public responsibility. The article proposes a shift from an ownership-centric imagination to a stewardship-and-access framework better suited to data-driven economies through doctrinal analysis, a comparative study of existing statutory and regulatory experiments, and an evaluation of institutional alternatives (including data trusts and access-oriented regulatory tools). The ultimate goal is practical: to identify legal interventions that maintain incentives for innovation while preventing enclosure and maintaining public interests.

CONCEPTUALISING DATA AS A LEGAL SUBJECT

There is a requirement of what Data actually represents in legal term in order to do a meaningful inquiry as to the existence or absence of intellectual property protection of data. Data doesn't exist in the single, stable category of traditional Intellectual objects but exist in multiple layers as the raw data is generated through discussions, interactions and related observations, processed data are arranged for practical use, and inferred data obtained by algorithmic analysis. Attempts to submit data to consistent proprietary treatment are complicated by the differences between each layer in terms of human intervention, economic worth, and legal relevance.

Data is increasingly being described as a crucial component of production from an economic standpoint, on par with labour or capital. Businesses that operate in digital markets gain a competitive edge from consistent access to big, varied, and constantly updated datasets rather than only from owning infrastructure or intellectual property. However, unlike traditional commodities, data is infinitely reproducible and non-rivalrous, so using it by one actor does not automatically reduce its availability to others. The notion of exclusivity that supports traditional intellectual property regimes is substantially undermined by this feature.[5]

[4] Hanyue Sun, Jiajia Li, Bingyuan Chen & Le Yang, Exploring Intellectual Property in the Digital Realm: A Bibliometric Study on Research on the Management and Protection of Data-Based Intellectual Property, 15 INFO. 780 (2024).
[5] Joshua Bishop Freeman & Louise Fresco, Governing the Data Commons: Policy, Practice, and the Advancement of Science, 47 INFO. MGMT. 237 (2010).

Additionally, data functions as a type of digital infrastructure. Access to data is becoming more and more necessary for meaningful engagement in markets, innovation ecosystems, and even democratic governance, much like highways or communication networks. Data is an enabling input rather than a final result in fields like public services, healthcare, finance, and artificial intelligence. By treating such infrastructure resources as privately held commodities, we run the risk of strengthening structural inequality, increasing hurdles to entry, and concentrating market power in the hands of those with the ability to gather and manage enormous amounts of data.

The idea of data as a commons contrasts with both infrastructure and commodity models. According to this perspective, shared access, reuse, and group benefit are what give data its social and economic value. The availability of data as a non-exclusive informational resource is essential to scientific study, public policy, journalism, and technological advancement. But there are drawbacks to a pure commons strategy, especially when it comes to accountability, quality control, and incentives for data collection. Unrestricted access could promote exploitative extraction without commensurate social benefit or deter investment in data-intensive enterprises. Divergent regulatory impulses are the result of this conceptual instability. On the one hand, governments are aware that unchecked data appropriation could reduce incentives to invest in infrastructure and data generation. However, granting ownership-like rights over data runs the risk of restricting informational resources that are essential for competitiveness, innovation, and research. As a result, data alternates between three opposing legal conceptions: as a commodity that can be traded, as digital infrastructure that is necessary for market participation, and as a commons whose social worth is found in shared access rather than exclusion.[6]

A deeper conflict between exclusivity and transparency in information governance is reflected in the challenge of integrating data into property-based legal frameworks. This conflict has historically been resolved by intellectual property law, which preserves the public domain of facts and ideas while restricting protection to particular types of intellectual effort. However, by creating value through aggregation, scalability, and analytics rather than through isolated acts of creativity or creation, data-driven economies obfuscate this distinction. As a result, the

[6] Jeffrey Ritter & Anna Mayer, Regulating Data as Property: A New Construct for Moving Forward, 16 DUKE L. & TECH. REV. 221 (2018).

lack of ownership over data is a symptom of IP law's core design assumptions being strained by modern technical realities rather than just a doctrinal gap.[7]

Therefore, it is necessary to go beyond the ownership versus non-ownership dichotomy in order to comprehend data as a legal entity. The main concern is not whether or if data should be owned, but rather how responsibility, control, and access to data should be organised to foster creativity while avoiding power consolidation. Before assessing why traditional IP regimes are unable to successfully regulate data and why informal mechanisms of control have emerged to fill the consequent governance vacuum, this conceptual reframing is crucial.

DATA AND TRADITIONAL IP REGIMES: DOCTRINAL INCOMPATIBILITY

On the surface, the intellectual property law may seem like a simple provision of ready-mapped instruments to guard precious resources. Copyright safeguarding of creativity, patents safeguarding of invention and trade secrets safeguarding of confidential business information. However, as we seek to insert data into these common structures the law starts to fail. This part gives a step-by-step account of why the traditional IP regimes fail to appreciate the fact that data can be a subject of protection by the law.

FIXATION AND ORIGINALITY: WHERE THIS ISSUE STARTS

The copyright law begins by a mere promise: make something original and fix it in a tangible form and the law will stand behind you. [8]However, this pledge will soon disintegrate in relation to data. The artistic or literary sense of creating most of the data is not provided to us, it is produced. The sensor measurements, transaction histories, user clicks, coordinates of locations, scientific measurements are produced by observing or by automatic processes, but not by human imaginative processes.[9] The copyright law does not even take into consideration labour alone as long as one develops such data with much effort and investment.

Originality has many times been noted by the courts to be the benchmark of protection rather than effort. This, in practice, implies that even a dataset of thousands or even millions of data points cannot be a copyrightable work merely because there are no creative decisions to make.[10] Fixation although generally occurred in digital databases does not save the assertion, fixation

[7] Josef Drexl, Designing Competitive Markets for Industrial Data-Between Propertization and Access, 8 J. INTELL. PROP. INFO. TECH. & E-COM. L. 257 (2017).
[8] Copyright Act of 1976, 17 U.S.C. § 102(a) (2018).
[9] Pamela Samuelson, Privacy as Intellectual Property?, 52 STAN. L. REV. 1125 (2000), https://people.ischool.berkeley.edu/~pam/papers/privasip_draft.pdf
[10] Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 347–48 (1991).

in the face of non-originality is immunologically impotent. This brings an uncomfortable fact: the information can be of the economic worth of gold, but cannot be captured by the law of copyright.

THE DOCTRINAL WALL OF THE FACTS-EXPRESSION DIVIDE

In order to see why the copyright law sets this line so solidly, one should resort to the facts-expression dichotomy. Copyright is not protection over ideas, but only protection over the expression of ideas.[11] Data by its very nature is on the side of facts. This principle was codified in the landmark case of *Feist Publications, Inc. v. Rural Telephone Service Co.* in which the U.S. Supreme Court said it had no reason to give copyright protection to a telephone directory, just because it contained true facts in an obvious way.

The morale of Feist spreads to the era of data economies readily. The law considers these as facts, which should be freely available to all regardless of whether the data is related to the consumer behaviour, weather patterns or the market prices. Copyright protection, should there be any, over data even in event where it is organised into compilations, only extends to the creative selection or arrangement, and not to the underlying data itself. Consequently, others can legitimately mining and re-using data provided they do not copy the expressive form of a safeguarded amassing.

On realising these inefficiencies, the European Union tried a legislative evasion by the sui generis database right. [12]This regime secures databases which have a heavy investment, even without originality. But this is by no means the end of the solution. The database right does not confer proprietorship in data, it only deters the removal or reuse of a considerable section of the database. In addition to this, empirical research indicates that the extra level of protection has not led to a rise in database creation, and may in fact lower access and competition.

Beyond the EU, the vast majority of other jurisdictions, such as India, have opted not to enact comparable systems, which supports the argument that copyright legislation, despite being enhanced, can only provide partial solutions to the data ownership problem.

WHY DATA IS NOT AN "INVENTION"

The story is different in the patent law- it is the story of technological advancement. In order

[11] Baker v. Selden, 101 U.S. 99, 102–04 (1880).
[12] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases, 1996 O.J. (L 77) 20.

to be eligible to be granted protection, an invention should be novel, non-obvious, and able to be industrialized. Data alone meets none of these conditions.[13] Courts, patent offices treat data as information born as opposed to invention. The law makes a defining line even in cases where the data is created by using advanced systems: the whole process can be patented, but not the data created.

Such a difference is particularly evident in the field of big data and artificial intelligence. Now, although algorithms, or data-processing techniques, can be patented, the data, which drives such systems, is not protected legally.

In patent laws like the European Union, patentability also requires given a technical effect. Information processing claims tend to fail here due to lack of a technical effect in hardware or system structure. This filter of the doctrine demonstrates a greater uneasiness with the act of giving monopolies on information. Information is perceived as an asset that should be utilized and not owned. Therefore, the law of patent excludes data systematically by the protection.[14]

It causes a dilemma even in the areas where the protection of patents is theoretically possible. In the case of patent law, a full disclosure of the invention is mandatory, which allows other people to duplicate the invention after the patent has expired. In the context of data-driven business, the disclosure can be interpreted as the release of valuable datasets - which kills competitive power. On the other hand, nondisclosure of data could make the patent inadequately revealed. With such a decision available, lots of companies simply do not participate in the patent system at all, which only supports the incompatibility between patent incentives and data governance.

ALTERNATIVE: THE LEAST CONCRETE BUT LEAST SOLID

It seems that the trade secret law can provide a solution. It secures information whose secrecy generates economic advantages and is liable to reasonable security precautions. Trade secrets do not require novelty or innovation as is the case with copyright and patents. It is this flexibility that makes trade secrecy an important tool to data-intensive firms.[15] Nonetheless, this security is conditional and weak. The moment data is in the air, it is lost regardless of the way of sharing and even leaks, reverse engineering. It is becoming hard to keep data confidential. The new data ecosystem is characterised by cloud storage, APIs, third party

[13] Patents Act, No. 39 of 1970, § 10 (India).
[14] Inge Graef, EU Competition Law, Data Protection and Online Platforms (Wolters Kluwer 2016).
[15] Unif. Trade Secrets Act § 1(4) (Unif. L. Comm'n 1985).

analytics and cross-border transfers. It is also difficult and expensive to establish misappropriation in these environments.

Besides, the trade secret law does not establish property rights with the rest of the world. It functions mostly based on contractual and relationship-based operations and this leaves loopholes in cases where data moves outside controlled environments. Excessive use of trade secrecy has wider implications. It promotes obscurity, interoperability, and constrained sharing of data that could otherwise be useful to innovation and research as well as competition. Effectively, secrecy constitutes an informal system of government, replacing the legality with the contractual regulation.

There is a definite story in all the three regimes. Copyright does not safeguard facts, but creativity. The protection of patent law is not information protection. Trade secret legislation does not provide openness, but secrecy. Information does not fit in any of these categories. This paradigm failure is the reason why data, though the foundation of the modern economies, is inequitably deprived of legal status as a type of property. Introducing impossibility of traditional IP law to handle data means the introduction of alternative governance frameworks, such as sui generis data rights, access regulation and frameworks of collective stewardship described later in this paper.

MECHANISMS OF INFORMAL OWNERSHIP/PRIVATE CONTROL

In case the traditional intellectual property law does not acknowledge data as property, the possession of data does not vanish. Rather, it is transferred to the extraterritoriality of law onto the plane of private ordering. Ideally, the control of data is not controlled by the legal rights of ownership, but rather controlled by contracts, platform regulations, and technological frameworks.

CONTRACTS AND LICENSING AGREEMENTS: CONTRACTS BY AGREEMENT

The control over data has been dominated by contracts as there are not statutory data ownership. The words ownership, exclusive rights, or perpetual licence are common to data-sharing agreements, SaaS contract, API licence and user agreements.[16] Doctrinally, these contracts fail to provide property rights to data against the world (erga omnes). They establish relational control instead, binding the parties only to the agreement. However, in practice, these contracts usually operate like conferred ownership particularly where the bargaining power is

[16] Morris R. Cohen, Property and Sovereignty, 13 CORNELL L.Q. 8 (1927).

asymmetric. As an illustration, companies often demand users to give extensive licences on user generated contents as the condition to access digital services. Although these licences are presented as consensual set-ups, they are not negotiable and are usually non-reciprocal. The outcome is a kind of contractual enclosure, and data are imprisoned behind legal walls without it being considered legal property. It is a contractualisation of the data governance, which gives the power to the privately drafted and enforced terms to the hands of private parties, rather than public institutions and courts.

There is no more apparent location of private control over data than in platform Terms of Service (ToS). Big digital platforms, i.e. social media corporations, commerce websites, search engine platforms, control large masses of data with standard-form contracts on millions of users. These terms often: have sweeping authority over user data, prohibit scraping, reusing or interoperability, allow one-sided changes in data policies, and restrict user remedies using arbitration product or jurisdiction clauses. Even though users are technically consenting to these conditions, actual consent is mostly just a fantasy.[17] Storytelling-wise, this is a legal sleight of hand, ownership is on one hand, whilst control is exercised on the other. Researchers have referred to platform governance as a type of private legislation wherein the rules which regulate the discourse and economic engagement of the population are established by the corporate players and not, as with a public law, by identifiable institutions charged with responsibility. Data within this constructs becomes a property subject to platform sovereignty as opposed to being a property subject to public law.

In addition to the use of contracts, technology itself is a decisive factor in data control. Access controls, encryption, application programming interfaces (APIs), digital rights management (DRM), and proprietary formats control the access to data, its consumption and terms and conditions. This is sometimes described as the manifestation of code is law, the notion that technological architecture can control behaviour even where the law allows it, technical barriers can make such rights meaningless in practice.[18] As an example, platforms can offer APIs which give partial or curated access to datasets, and hold entire datasets internally. Instead, others use encryption or rate-limiting to avoid analysis or competition by the third party. The anti-circumvention laws will be a legal reinforcement of these controls, further consolidating the private control.

[17] Julie E. Cohen, Law for the Platform Economy, 51 U.C. DAVIS L. REV. 133 (2017).
[18] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 6–8 (Basic Books 1999).

DEMOCRATIC AND OPENNESS ISSUES

The overall impact is the establishment of a system in which control is a by-product of design decisions instead of legal rights, which brings the issue of transparency, accountability, and equity up. The emergence of informal data ownership systems can have a wider scope than commercial interests. In the event that data governance is conducted by contracts and code mostly, it circumvents popular will and the rule of law.

This is incredibly vexing in the situations where data is involved in: public discourse, electoral processes, availability of basic services, decision-making, and algorithmic decision-making. AI training and deployment. The private possession of data with social significance may limit research and journalism and supervision, whereas in contrast to statutory IP regimes, which are constrained by constitutional boundaries, exceptions, and protection of the public interest, there are no established mechanisms in place to balance competing interests in private ordering.[19] Practically, the lack of legal title ownership rights has failed to bring about transparency. Rather, it has generated disjointed, cloudy and power-coded systems of control, that have brought more questions than solutions, that data governance is being determined by markets and not the law.

MARKET POWER, COMPETITION, AND THE POLITICAL ECONOMY OF DATA CONTROL

Market structure and competitiveness are significantly impacted by the transition from formal intellectual property regimes to unofficial data control methods. Although the lack of ownership-based intellectual property rights over data may at first seem to maintain transparency, in reality it has made it easier for those with the ability to maintain long-term control over massive databases to amass economic power. Thus, data-driven markets highlight a structural paradox: data is both economically exclusive and legally non-proprietary.[20]

Data asymmetry is at the heart of this issue. Businesses that amass large datasets profit from feedback cycles whereby data makes better products possible, better products draw in more customers, and more users produce even more data. Regardless of their technological proficiency or potential for innovation, this self-reinforcing dynamic creates significant entry

[19] SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 93–95 (PublicAffairs 2019).
[20] Wolfgang Kerber, Digital Markets, Data, and Privacy: Competition Law, Consumer Law and Data Protection, 11 J. INTELL. PROP. L. & PRAC. 856 (2016).

barriers for new and smaller businesses without comparable access to data. Data-based barriers, in contrast to traditional capital-intensive barriers, are frequently imperceptible, hard to measure, and difficult to replicate, solidifying incumbent dominance without overt legal exclusivity.

These characteristics have proven difficult for competition law to adequately address. Price impacts, market shares, and consumer harm are the main emphasis of traditional antitrust study; these measures frequently fall short of capturing the competitive relevance of data accumulation. In many digital markets, services are provided for free, and there is competition based on factors like quality, personalisation, and innovation speed, all of which are directly related to data access. Therefore, monopolistic outcomes are not prevented by the lack of formal IP protection over data; rather, they are concealed behind supposedly open informational resources.[21]

This image is further complicated by the political economy of data control. In addition to competing inside markets, dominant platforms are increasingly taking on the role of market governors by establishing the parameters for data access, sharing, and reuse. These entities influence downstream innovation ecosystems through contractual limitations, interoperability constraints, and limited access through application programming interfaces. Because they frequently continue to rely on platform-controlled data infrastructures, smaller businesses, researchers, and public institutions are susceptible to unilateral changes in access terms. This type of private governance essentially replaces corporate discretion with public regulatory monitoring.

There are serious normative issues with this concentration of power. Data control takes on a quasi-public nature when access to data dictates the capacity to innovate, engage in markets, or examine algorithmic decision-making. However, data-rich platforms function without commensurate duties of neutrality, transparency, or accountability, in contrast to conventional public utilities or regulated monopolies. As a result, there is a governance gap where the checks and balances usually associated with property rights or regulatory systems are not present, allowing economic control over data to convert into social and political influence.[22]

Furthermore, global inequality is made worse by the concentration of data. While actors in

[21] Heike Schweitzer, Martin Peitz & Wolfgang Kerber, Data Access, Consumer Interests and Public Welfare, MAX PLANCK INST. FOR INNOVATION & COMPETITION RSCH. PAPER NO. 18-03 (2018).
[22] Hal R. Varian, Market Power in the Digital Economy, SSRN (2019), https://ssrn.com/abstract=3123957

emerging economies frequently operate as data suppliers rather than recipients, companies with their headquarters in data-rich jurisdictions are better positioned to derive value from cross-border data flows. Data-driven value creation runs the risk of becoming extractive rather than inclusive in the absence of strong governance systems, which would exacerbate already-existing disparities in economic and technological power.[23]

These developments show that the crisis of data governance encompasses more general issues of market regulation and economic justice rather than merely doctrinal flaws in IP law. The structural factors that allow concentration and exclusion are not addressed when data is just treated as an object of private control, whether through contracts or technological obstacles. This realisation emphasises the necessity of governance frameworks that directly address the competitive significance of data instead of depending on ownership paradigms that are inappropriate for its economic realities.

TOWARDS A GOVERNANCE FRAMEWORK FOR DATA: COMPARATIVE LESSONS AND REFORM PROPOSALS

The preceding analysis shows that applying conventional intellectual property concepts to data would not alleviate the dilemma of "data without ownership." A deeper governance deficit rather than a simple lack of proprietary rights is revealed by the failure of copyright, patent, and trade secret regimes as well as the emergence of unofficial private control. A regulatory movement away from ownership-centric solutions and towards frameworks that organise access, control, and responsibility in a way that is sensitive to the distinct economic and social aspects of data is necessary to address this deficit. Scholarly proposals and comparative experiences provide important direction for building such a framework.

The replacement of blanket ownership with customised access rights has been a notable response. Jurisdictions are realising more and more that the conditions under which access is allowed or restricted, rather than exclusivity, are what give data its competitive worth. Reducing data asymmetries without diminishing incentives for data generation is the goal of tools like data portability, interoperability requirements, and regulated access for downstream innovation. Access-based models, in contrast to proprietary rights, aim to maintain market contestability by prohibiting incumbents from utilising data control as a means of exclusion.

[23] Daniel J. Gervais, Exploring the Interfaces Between Big Data and Intellectual Property Law, 14 J. INTELL. PROP. L. & PRAC. 178 (2019).

Crucially, these responsibilities must continue to be sector-specific and calibrated because indiscriminate data sharing jeopardises security, privacy, and legitimate business interests.

With its sui generis database right, which is intended to safeguard significant investment in data compilation regardless of originality, the European Database Directive represents a more ownership-adjacent experiment. However, a thorough analysis by scholars has revealed that this system may constrain competition and access while providing little advantages for innovation. Its experience highlights an important lesson: any sui generis data protection must be strictly defined, time-bound, and subject to significant exceptions. Instead of acknowledging ownership of the data itself, a well-crafted regulation may prevent the widespread appropriation of datasets for a brief period of time while maintaining the ability to reuse individual data points and guaranteeing strong research and exemptions for the public interest. By taking a cautious approach, the extremes of IP maximalism are avoided.

Scholars are increasingly promoting institutional governance methods, including data stewardship and data trusts, in addition to private and access-based procedures. Instead of viewing data control as a proprietary right, these frameworks rethink it as a fiduciary duty. Accredited intermediaries maintain and administer datasets under stewardship models on behalf of users, contributors, or the general public, subject to legal obligations of responsibility, transparency, and purpose limitation. By integrating decision-making into regulated institutions, this collective governance system lessens dependency on bilateral contracts and mitigates power disparities. Although promising, the successful implementation of stewardship models necessitates legal acknowledgement, unambiguous governance requirements, and protections against regulatory capture.

In order to address data concentration, competition law is also essential. Conventional antitrust instruments, which are mainly concerned with price impacts, are frequently inadequate for identifying the negative effects of data-driven exclusion in zero-price markets. A more comprehensive strategy that considers data-driven foreclosure tactics, interoperability limitations, and access denials as possible causes of anticompetitive harm is supported by current research. In these situations, behavioural interventions like required interoperability or access commitments should take precedence over structural disruptions as remedies. Competition authorities must be cautious, though, and make sure that any forced access to data is reasonable, complying with privacy laws, and technically possible.

Without technical interoperability standards, legal entitlements are insufficient on their own.

Without common formats, APIs, and metadata standards that allow for meaningful reuse, data access rights become practically meaningless. The significance of combining legal requirements with technical specifications created through multi-stakeholder processes is emphasised by comparative regulatory initiatives. These standards lower transaction costs, improve compliance, and stop powerful players from using technical design decisions to undermine access. To avoid private capture and guarantee consistency with more general policy goals, public scrutiny of standard-setting is crucial.

Security and privacy measures must be incorporated into every governance system as fundamental, not incidental, factors. Without sufficient controls, data-sharing responsibilities run the danger of making surveillance, re-identification, and misuse worse. Access regimes should include auditability, security certifications, purpose limitation, and appropriate anonymisation methods, according to scholarly consensus. These precautions are essential to preserving public confidence and preventing unforeseen societal harm from governance improvements.

Lastly, sector-sensitive and flexible regulation is required due to data heterogeneity. The sensitivity, economic function, and social influence of data vary greatly between situations, including public administration, health, finance, and transportation. Thus, a one-size-fits-all strategy is not feasible. More accuracy and legitimacy are provided by graduated regulatory frameworks that differentiate between personal and non-personal data, high-risk and low-risk datasets, and commercial and public-interest usage. Sunset provisions and regular review procedures further guarantee that governance systems continue to adapt to empirical data and technological advancements.

When combined, these comparative lessons imply that data governance in data-driven economies should reject both extremes: total data propertisation and total regulatory disregard. Rather, a more logical and acceptable solution is provided by a hybrid framework that combines institutional stewardship, competition-aware remedies, calibrated access rights, narrowly targeted protective measures, technical interoperability, and strong safeguards. Such a framework preserves innovation, competition, and the public interest goals that traditional intellectual property regimes alone are ill-suited to achieve while bringing legal regulation into line with the material reality of data.

IS SUI GENERIS DATA THE CORRECT SOLUTION?

Having already traced the recurrent failure of the conventional intellectual property regimes to

adapt to data, one might then ask: in the event that copyright, patent, and trade secret law are unsuitable to data, would the law not then establish a new protection regime altogether? This is the question that has been at the centre of the modern discussion of data governance, and has prompted a range of scholars and policy-makers to suggest a sui generis data right the legal regime specific to the special nature of data. The attractiveness of such a solution is self-evident, at first. Digital economies are now run on data, but it is not being adequately safeguarded as a legal property.

A sui generis right is an assuring, definite and incentive-driven right. The common argument of proponents of a sui generis data right will start with a fairly straightforward fairness argument: companies and organizations place vast resources in the collection, cleaning, verification, and maintenance of datasets, yet under the law they are not entitled to keep off competitors taking advantage of the economic benefits of their investments.[24] Unlike creative works or technical inventions, data producers frequently have no power to prevent competitors to take advantage of economic benefits of their investments. In that sense, a committed data right would operate a lot like customary IP regimes- it would eliminate market failures by internalising investment incentives. Through a limited exclusivity, the law may induce the creation of quality datasets especially in fields like healthcare, finance, transport and scientific study.

The second argument in support of sui generis protection is the issue of legal certainty. Currently, contracts, licensing agreements and technological controls are crucial in data governance. Such mechanisms work differently across jurisdictions and usually favour mighty market players.[25] A statutory data right would be useful in standardising protection and lowering the transactional cost by explicitly stipulating who should possess or restrict access to or make profit out of data. In the case of emerging economies and cross-border data markets, such transparency is usually sold as the key to encouraging investment and trust. Other academics suggest that the lack of official rights of data does the reverse and makes the market more concentrated. Big platforms, which have the capacity to impose contractual and technical constraints, de facto owns data without having to face any significant public scrutiny, A sui generis regime, it is argued, may bring such control into a regulated framework, making exclusivity transparent and limited by statute.

[24] European Commission, Building a European Data Economy, COM (2017) 9 final (Jan. 10, 2017).
[25] Julie E. Cohen, Law for the Platform Economy, 51 U.C. DAVIS L. REV. 133, 204 (2017).

HAZARDS OF DATA ENCLOSURE AND OVER-PROTECTION

Nevertheless, the sui generis data right proposal has received a lot of criticism despite such arguments. Risk of over-propertisation- the metamorphosis of data into an exclusionary commodity that is like land or chattels is the most noteworthy.

Information, as compared to conventional IP subject matter, frequently finds its worth in aggregation, reuse, as well as recombination. Giving access to data on a basis of exclusive rights will mean putting in an information common that has hitherto served as a source of information.[26] Researchers caution firm data rights might suppress future innovations, limit research and access to socially desirable information. The case with the EU Database Directive is an example to be warned about. Although this is meant to encourage investments, empirical research findings indicate that this has not been successful and could have even deterred the reuse of data without necessarily driving a higher production in the database.

Exceptional data rights may be overly broad and overly expansive concerning public-interest activities. Journalistic inquiries, scholarly studies as well as development of AI often depend on availability of extensive datasets. In case proprietary rights were placed on the data, such activities may be more expensive, subject to legal confusion, or even excluded altogether. This is a burning issue in the AI environment. The large-scale models require the availability of various and wide-ranging datasets in order to train them. The fractured state of data ownership might commit to entrenchment by dominant actors and at the expense of smaller innovators and state institutions.

Paradoxically, a sui generis data right can support the inequalities it is trying to address. The big corporations are more in a position to register, enforce, and litigate on the rights to data than small firms and individuals might be able to. The outcome might be the increased consolidation of data markets instead of democratizing them.

OTHER MODELS: NOT JUST EXCLUSIVE OWNERSHIP

Having realised these dangers, numerous academics also suggest that the solution is not in ownership-based rights, but in access-based models of governance. Instead of exclusivity, the law may be aimed at providing fair data access. The data protection regimes of some countries already have the data portability rights, which would allow users to transfer data across

[26] James Boyle, The Second Enclosure Movement and the Construction of the Public Domain, 66 LAW & CONTEMP. PROBS. 33 (2003).

platforms to decrease the lock-in effect and enhance competition.[27] The difference in such approaches is that it does not emphasize ownership but mobilizes and regulates.

The second option is obligatory data sharing on controlled terms, especially in the fields, which are defined by high network effects. The access to data is becoming a more popular curative to market dominance of competitive authorities implying that the regulation can be more efficient than proprietary rights.[28]

Lastly, there are also the scholars who propose that data should be considered a controlled property and not a personal one. This model is based on the idea that the tools of the public law, competition law, data protection law and industry-specific regulation are at the heart of the control of access, usage, and responsibility.[29]

The controversy of a sui generis right in data right eventually leads to the more fundamental issue: what is data as a resource? When data is considered as property, exclusivity is a natural result. When it is approached as infrastructure or a common social good, governance has to be access oriented, just, and in the interest of the people.

This discussion indicates that although a sui generis data right seems to provide an intuitively attractive answer, it will recycle the errors of current IP regimes the replacement of one kind of a doctrinal mismatch with another. The problem, then, is not with the establishment of more powerful ownership claims, but with the establishment of new forms of governance that demonstrate the economic and social peculiarities of data.

DISCUSSION AND FUTURE RESEARCH

This paper started with a basic, but disturbing fact: data has become one of the most valuable assets of the contemporary economy, and it is still legally inaccessible. In industries, including those of finances, healthcare, governments, artificial intelligence, and online platforms, data is the catalyst of innovation, market dominance, and decision-making. Even with this centrality, the law has not been able to define what data is legally what is legal and who is supposed to control it.

[27] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), art. 20, 2016 O.J. (L 119) 1.
[28] ORG. FOR ECON. CO-OPERATION & DEV., DATA-DRIVEN INNOVATION: BIG DATA FOR GROWTH AND WELL-BEING (OECD Publ'g 2015), https://www.oecd.org/innovation/data-driven-innovation-9789264229358-en.htm
[29] JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM (Oxford Univ. Press 2019).

Traditional intellectual property regimes analysis indicates that this battle is structural rather than accidental. The copyright law was not meant to safeguard information, but creativity. The fact that it insists on originality and its strict distinction between data and expression makes sure that the data, however valuable, will not fall under its preserving power. In its turn, patent law is an invention that rewards technical invention and requires disclosure, which is why it is not the most suitable means of safeguarding datasets that are not technological solutions, but informational inputs. The law of trade secrets provides conditional protection but at the price of secrecy, weakness and obscurity. The combination of these regimes reveals the constraints of an IP system designed in an industrial and creative economy and now expected to regulate a data-driven one.

Lack of IP protection based on ownership has not caused the law to become neutral. Rather it has facilitated the emergence of privatized modes of control, in the form of contracts, terms of use of platforms, and technological enclosures, which have become de facto property regimes. Such mechanisms tend to concentrate power in the control of those holding large amounts of data, increase information asymmetry and create serious concerns over transparency, competition and democratic accountability. In this regard, the absence of legal status of data has not stopped the exclusivity; it has simply just transferred the power of the law to the hands of the private ordering. A comparative analysis also highlights the ineffectiveness of the current methods. The sui generis database right of the European Union shows not only the attractiveness but also the dangers of establishing new proprietary interests on data. Although it attempts to incentivize investment, its weak performance and the probable limitations that it imposes on access warn of a blindly broadening of the data property rights. The market-based paradigm used in the United States, in turn, prioritizes competition and innovation, but does not always deal with data concentration and power imbalances. The new forms of governance especially in China are emphasizing the effects of state centricity of exerting strategic interests and at the same time has brought up the issue of surveillance and personal privacy.

This paper advises that in its review of the boundaries of intellectual property law, data governance cannot be confined to the dichotomy of ownership and no protection. The problem is how to create the laws that keep the access open and still do not reduce the innovation, and allocate the gains of data-based economies more fairly. In the case of jurisdictions such as India and other emerging economies, this is an especially pressing thing to do as the policy decisions in the field of data today determine the digital sovereignty, economic development, and personal rights over decades to come. It is a matter of change in the end the story of data and

intellectual property. Due to the changing nature of economies, legal categories have to change as well. The awareness of the inefficiency of conventional IP regimes is no failure of law but an opportunity to reinvent it, developing governance frameworks that are responsive to the realities of the digital era whilst retaining some touch with the values of fairness, access and the common good.