Academic Journal of Humanities & Social Sciences
ISSN 2616-5783 Vol.7, Issue 2: 279-288, DOI: 10.25236/AJHSS.2024.070240

Paradigm shift of commercial data protection: From an IP approach to a *sui generis* approach

Haodi Deng

Melbourne Law School, The University of Melbourne, Melbourne, Australia

Abstract: *Commercial data has similar features to IP subject matters such as intangibility, non-rivalry, non-exclusivity, and non-expendability, which underpin commercial data protection under the IP regime. By extending existing IP subjects to include commercial data, the established IP regime is capable of protecting commercial data. However, such an approach is difficult to provide adequate protection for commercial data, which has features that distinguish it from IP subject matters. This article contends a new approach is needed to commercial data protection. Compared with protecting commercial data as novel subject matter under the IP regime, this article favors establishing a sui generis property regime for commercial data, drawing on the rationale and normative design of the IP regime. Using the IP regime as a guide, specific rules regarding the content of rights, the duration of protection, and the subject matter of commercial data protection can be designed. Further, a mechanism for balancing interests can be established by introducing fair dealing exceptions and FRAND principles to the commercial data property regime.*

Keywords: *Commercial Data; Intellectual Property; Paradigm Shift; Sui Generis Approach*

1. Introduction

The term "commercial data" was introduced to distinguish between personal data and data resources that result from the processing of massive amounts of data by market entities. Cloud computing, AI, and other technologies have made commercial data a strategic resource for companies seeking to increase their market share and improve their competitive position. Companies have an urgent need to protect the interests carried by their commercial data. As a result, the question of how to protect the interests carried by commercial data under the existing legal framework has become a critical concern in a data-driven economy.

Part 2 sketches the features of commercial data while comparing them to those of IP subject matters. It concludes that although commercial data shares some similarities (e.g. intangibility) with IP subject matters, it is distinctive in terms of quantity, type, and dynamic.

Part 3 analyzes the extent to which the existing IP regime protects commercial data. It argues that the existing IP regime can protect commercial data by extending existing IP subject matters (e.g. works and trade secrets) to include commercial data. This protection, however, is insufficient.

Part 4 contends that establishing of a *sui generis* property regime around commercial data is more advantageous than protecting commercial data as a novel subject matter under the IP regime. It proposes the *sui generis* property regime by drawing lessons from the IP regime.

2. The features of commercial data

2.1. The similar features to subject matters of IP

The term 'Intellectual Property' refers to a wide range of intangible subject matters protected by a loose collection of legal titles[1]. The features of these subject matters include intangibility, non-rivalry, non-exclusivity and non-expendability. In comparing commercial data with IP subject matters, one can observe some similarities. These similarities are the basis for commercial data protection within the IP regime.

2.1.1. Intangible

Commercial data has an intangible nature. In essence, commercial data consists of strings of 0 and 1

ISSN 2616-5783 Vol.7, Issue 2: 279-288, DOI: 10.25236/AJHSS.2024.070240

encoded in binary format and stored on a specific storage device for computer recognition and processing[2]. Commercial data does not have a material form in the physical sense and cannot be tangibly controlled or possessed by any person. Compared to tangible property, commercial data is more closely akin to intangible property, such as subject matters of IP.

2.1.2. Non-rivalrous and Non-excludable

Commercial data demonstrates the feature of non-rivalry. Commercial data can be processed and analyzed jointly by multiple persons at the same time, or used repeatedly by the same person. The increase in the number of users, the accumulation of usage, and the change in the manner of use do not diminish the quality and usefulness of commercial data. Therefore, data sharing may not encounter the issues of competition associated with finite resources. In addition, commercial data shows a prominent non-exclusive character. The enjoyment of commercial data by one person does not prevent others from enjoying it. This means that without government-backed exclusive rights being granted, the original controller of commercial data usually cannot exclude others from the use of that data once made public. This non-exclusive feature becomes even more apparent in the context of Big Data due to the low cost of replicating commercial data.

2.1.3. Non-expendable

Lastly, commercial data presents a feature of non-expendability. Commercial data is not subject to physical wear and tear as a result of use, let alone loss in the course of delivery of goods and transfer of property. Theoretically, commercial data can exist permanently once it has been created. Accordingly, the risk of loss normally faced by tangible objects does not exist for commercial data. As for the commercial data widely available on the internet, the data itself will not be altered or changed regardless of whether the medium on which the data is stored is damaged or lost. In short, commercial data is similar to IP subject matters, reflecting its non-expendable feature.

2.2. The distinctive features of commercial data

Commercial data, as a newly emerging factor of production in the era of big data, has some features distinct from IP subject matters. These features require special attention since they may present dilemmas for commercial data protection within the existing intellectual property regime. Compared with the subject matters of IP, commercial data is distinctive in terms of quantity, type and dynamics.

2.2.1. Enormous quantities

In the era of big data, only massive quantities of data can accurately reflect the macro market, which is capable of assisting companies in making commercial decisions objectively and comprehensively, and generating any real economic benefit. Article 2(7) of the Japanese *Unfair Competition Prevention Act*, which defines shared data, emphasizes that shared data should be "accumulated to a significant extent"[3]. The majority of commercial data is in the form of sets containing a substantial quantity of single data elements. This is significantly different from the subject matters of IP, which normally exists in a single form. This difference may create theoretical and practical difficulties in protecting commercial data under the existing IP regime. For one thing, some may argue that commercial data does not have the scarcity of property, given its enormous quantities. If this were the case, there would be no basis for employing the intellectual property regime to protect commercial data which is not property. This argument, however, may be one-sided. Even though data is non-expendable, its economic value is still discernible and scarce, taking into account both the cost of collecting the data as well as the ability of data processors to mine and analyze it. This is evidenced by the frequent occurrence of improperly grabbed and misappropriated commercial data, which indicates that the demand for commercial data is not sufficiently met and that commercial data resources are being allocated in a polarized manner[4]. For another, a substantial increase in transaction costs in the data sector is also likely to result from enormous quantities of commercial data. How to solve this problem by employing the property rights regime needs to be further considered by policymakers.

2.2.2. Diverse types

Commercial data can be classified into various types based on different classification criteria. For example, commercial data can be divided into public data and non-public data based on the degree of publicity of the data. Depending on the scenarios in which the data is being used, commercial data can include scientific data, government data and company data. These different types of commercial data carry different values that reflect varying demands for the protection of interests. Therefore, the construction of the commercial data protection system should take into account the diversity of

ISSN 2616-5783 Vol.7, Issue 2: 279-288, DOI: 10.25236/AJHSS.2024.070240

commercial data types and, on the basis of recognizing their common features, allocate differentiated entitlements to those different types of commercial data. Otherwise, the indiscriminate inclusion of different types of commercial data in a specific intellectual property regime and the ignorance of their distinctions will result in the loss of operability of the regime for the protection of commercial data.

2.2.3. Dynamic

The processing of commercial data includes multiple stages of collection, storage, use, and transmission[5]. Data processors at different stages of the processing can carry out further uses of data and innovation activities based on the commercial data of others. This means that the form and attributes of commercial data are constantly changing during the processing of data. Meanwhile, the dynamic feature of commercial data is also reflected in its continuous self-renewal. In the era of big data, the scale of data grows at an explosive rate, to the extent that billions of pieces of content are generated on the Internet at every second. This means that even in the course of the collection of raw data, the content of commercial data undergoes continuous additions, deletions and alterations, which usually result in some degree of change to the commercial data. This frequently occurring self-renewal may pose challenges to the inclusion of commercial data into the established regime of IP subject matters. This dynamic feature of the data attracted the attention of the drafters of the *EU Database Directive 96/9/EC* ("the EU Database Directive"), which made special provision in terms of the duration of protection in cases of "any substantial change, evaluated qualitatively or quantitatively, to the contents of a database"[6].

3. The approach within IP regimes of commercial data protection

Commercial data and IP subject matters share similarities while the purposes of their protection overlap in several aspects. In this regard, it is reasonable to protect commercial data under the IP regime. Commercial data can be protected under the existing IP regime through specific IP rights (e.g. copyrights, patent rights), database *sui generis* rights, and anti-unfair competition. These avenues, however, may not provide sufficient protection due to the distinctive features of commercial data.

3.1. Copyright Protection

To attract protection under the Australian *Copyright Act*, a work must fall within one of the categories of protectable subject matter. Among these protectable subject matters are literary works including compilations[7]. A compilation must be original (as well as satisfy the requirements for connecting factors and material form) to meet the criteria for protection. The originality of a compilation is reflected in the selection and arrangement of information[8]. Therefore, commercial data may be protected by copyright as a compilation if its selection or arrangement is original.

On the other hand, commercial data protection under the copyright regime may face some difficulties, mainly in two aspects.

For one thing, commercial data may have difficulty in meeting the originality requirement. Originality is a threshold requirement for subsistence of copyright in Part III works. In contrast to compilations, commercial data is more concerned with the comprehensiveness and quantity of data than with the arrangement or selection of data[9]. One of the most significant features of commercial data is its enormous quantity. Commercial data is usually generated automatically by defined algorithms, classified and organized according to standards recognizable by computer systems. Such nearly entirely automated data collection activities hardly satisfy the originality requirement for compilations. Consequently, a significant body of commercial data may not be eligible for copyright protection due to lack of originality.

For another, commercial data itself may not be protected by copyright according to the principle of idea-expression dichotomy. Copyright protection covers the selection and arrangement of a compilation (a particular form of expression), but does not extend to information itself (an idea). Accordingly, the copyright regime can protect the original selection and arrangement of commercial data, rather than the data itself. In other words, even if copyright is granted to a commercial data controller, the controller is not entitled to prevent others from using the commercial data itself. The conduct of data-grabbing will not constitute copyright infringement if simple modifications are made to the original selection and arrangement of commercial data in collecting or using. In this sense, commercial data protection under the copyright regime has limitations.

ISSN 2616-5783 Vol.7, Issue 2: 279-288, DOI: 10.25236/AJHSS.2024.070240

3.2. Patent Protection

The main approach to protecting commercial data under the patent regime is to apply for patents on commercial data-related technologies. Computer devices, artificial intelligence, algorithms and other technologies are closely related to the collection and processing of commercial data. Among these technologies, some technical solutions applying the laws of nature to address specific technical issues are patentable, which may be eligible for patent protection. If commercial data-related techniques were patented, others would be restricted to processing data, protecting commercial data *de facto*.

Nevertheless, the protection of commercial data under the patent regime has some limitations.

Firstly, a substantial amount of commercial data-related technology may not be eligible for patent protection due to a lack of patentability. In *Alice Corp v. CLS Bank*, for example, the US court denied the patentability of a big data-related program on the basis that it is an abstract idea and algorithm running on a machine, which is not a patent-eligible invention[10]. Likewise, Article 25(2) of the Chinese *Patent Law* explicitly excludes "rules and methods for mental activity" from patentable subject matters[11]. Some algorithms and computer programs related to commercial data may be regarded as "rules and methods of mental activity". This means that these commercial data-related technologies may not be patentable under Chinese *Patent Law*. Moreover, commercial data-related technologies might be difficult to be considered as patentable invention as they are hardly distinguished from unpatentable natural laws. For example, the US court in *Mayo v Prometheus* held that a diagnostic technique related to big data was not patentable since it was a natural law[12]. The examples above demonstrate the difficulty of patenting commercial data-related technologies in the jurisdictions mentioned.

Secondly, some commercial data-related technologies may not meet the requirements for patent validity. The requirements for patent validity under the Australian patent regime are similar to those of most other countries as a result of the *TRIPS Agreement* as well as other international agreement. Article 27 of the *TRIPS Agreement* provides that patents may be granted for any invention, provided that it is new, involves an inventive step, and allows for industrial application[13]. As patents confer strong exclusive rights, patent validity requirements are usually strict to balance the interests of the patentee and the public. The strict requirements may deter most companies from seeking patent protection for commercial data. In the US, where the digital economy flourishes, most participants in the data sector tend to protect commercial data through trade secrets rather than applying for patents[14]. A possible explanation is that the threshold for a valid patent is too high, with too small a chance of obtaining one.

3.3. Trade Secrets

Generally, trade secrets refer to business information that is not known to the public, has a commercial value, and is protected by appropriate measures by the controller, which falls under the concept of 'undisclosed information' in Article 39 of the *TRIPS Agreement*[15]. Undisclosed commercial data is not known to the public, and has commercial value in terms of providing competitive advantages. Furthermore, by using technical measures such as authentication and digital encryption, which can prevent other companies from obtaining and accessing commercial data, companies can obtain *de facto* control over commercial data. Therefore, commercial data with commercial value that is not publicly available and for which reasonable measures have been taken to protect its secrecy may be protected as trade secrets. Under Article 4 of the *Data Act* proposed by the European Commission, all specific necessary measures should be taken to protect the confidentiality of shared data[16]. Although the *Data Act* does not confer a new right on data controllers, it recognizes that data controllers have effective control over their data in practice.

While protecting commercial data through trade secrets is more effective than patents, this avenue does not satisfy companies' demand to protect commercial data. This is because trade secrets essentially serve as a means of maintaining market order that cannot provide adequate protection for commercial data. The exercise of the rights conferred by trade secrets is conditional upon disclosure, acquisition, or use by others through unfair means, or subsequent disclosure in breach of faith after it has already been legitimately known[17]. This means that, except in these cases, companies cannot protect commercial data through trade secrets. For example, the acquisition of raw data through reverse engineering does not infringe trade secrets. Moreover, the widespread use of cloud storage technology also makes it possible to obtain companies' raw data directly through legitimate channels by accessing cloud platforms. Such raw data are not trade secrets since they are publicly known.

ISSN 2616-5783 Vol.7, Issue 2: 279-288, DOI: 10.25236/AJHSS.2024.070240

The disadvantage of protecting commercial data by trade secrets lies in the potential monopoly of data as a result of the objection to disclosure. Trade secrets protection indirectly encourages companies to withhold commercial data under their control, which would result in a reduction in data resources available on the market. Furthermore, the monopoly of commercial data prevents other companies from mining and analyzing the data, resulting in their meaningless repetitive work, thereby reducing innovative activities in the data industry. Moreover, the monopoly of commercial data will hinder the normal development of the data industry. For one thing, protecting commercial data as trade secrets will substantially increase transaction costs. This is because companies would need to invest in maintaining the confidentiality of their commercial data. To prevent data from entering the public domain, companies may not only need to invest additional funds in developing and implementing technical measures such as digital encryption and authentication, but they may also need to enter into additional non-disclosure agreements with users when providing commercial data. For another, the monopoly of commercial data can hinder the realization of its economic value. The most prominent characteristic of the digital economy is data sharing. The economic value of data can only be fully realized through its use and sharing. The trade secrets protection system, however, emphasizes monopoly rather than sharing, which is contrary to the objectives of the digital economy.

3.4. Sui generis database right protection

The EU Database Directive is concerned with original databases and non-original databases[18]. A parallel legal protection system of copyright and *sui generis* right for databases was established by the EU Database Directive, whereby original databases are protected by copyright, while non-original databases by a *sui generis* right. Under the EU Database Directive, a non-original database is an "object of protection" if its maker has made a "substantial investment". Therefore, the EU Database Directive protects the substantial investment made by a maker to produce a non-original database, i.e. the maker's labour. Similarly, Germany, a member of the EU, protects non-original database makers' fruits of labour by 'neighbouring rights' under the *Act on Copyright and Related Rights*. Under Section 87b of the Act, producers of databases have the exclusive right to distribute, reproduce and communicate databases to the public[19].

By creating a *sui generis* right, the EU has overcome the difficulty of protecting publicly available and non-original databases. There are, however, limitations to commercial data protection in this way. For one thing, commercial data is significantly different from databases in terms of scale and structure. These differences between commercial data and databases grow ever larger in the era of big data. This makes it difficult to extend the *sui generis* database right protection to commercial data. For another, the avenue of protecting commercial data through a *sui generis* right may be infeasible in jurisdictions without legislation similar to the Database Directive that grants a sui generis right to makers of non-original databases. For example, at nearly the same time that the EU Database Directive was enacted, there was a heated debate in the United States Congress about special protection for databases, during which several versions of proposed legislation on special protection for databases were introduced. These proposals, however, were ultimately shelved due to strong opposition from the scientific community and the networking industry[20]. Therefore, makers of non-original databases in the US are not entitled to *sui generis* rights. Nevertheless, the idea of creating a *sui generis* right to extend protection beyond traditional IP regime is instructive. In cases where existing IP regime fails to provide adequate protection for commercial data, a *sui generis* right may be necessary.

3.5. Anti-unfair Competition

In the US, misappropriation of information may constitute unfair competition[21]. The unfair competitive advantage obtained by commercial competitors in the market through free-riding on consumer goods from others will harm the legitimate interests of other competitors with adverse effects on competition in the market, which ultimately affects consumers' welfare. In this context, the misappropriation doctrine was created in judicial practice with the aim of defending the legitimate interests of competitors and protecting goods that fell outside the scope of statutory IP protection.

The misappropriation doctrine originated from *INS v AP*[22]. The court in this case held that copyright does not subsist in news matters which are public property. It was held, however, that news collection and transmission require labor and money expenditures, and therefore should be protected as "quasi property" under anti-unfair competition law. Since then, the court in *NBA v. Motorola* has refined the scope and rules of application of the doctrine[23]. The court in this case introduced the five-factor test for misappropriation doctrine, which includes that the information misappropriated is

ISSN 2616-5783 Vol.7, Issue 2: 279-288, DOI: 10.25236/AJHSS.2024.070240

time-sensitive and that the defendant's misappropriation directly competes with the product or service provided by the plaintiff. Although the misappropriation principle was originally applied primarily to hot news, it has been extended to other areas in recent years. For example, the court in *Facebook v ConnectU* applied the doctrine to user information on social media sites[24]. Similarly, the court in Banxcorp v Costco applied the doctrine to financial information[25]. Moreover, in *hiQ Labs v LinkedIn*, the court held that the misappropriation doctrine may be an available remedy for market participants who considered themselves harmed by data-grabbing[26]. Overall, the misappropriation doctrine can now be used to protect commercial data.

On the other hand, the misappropriation doctrine has difficulties in protecting commercial data. This may render the doctrine only a temporary resort to commercial data protection.

First, the misappropriation doctrine has a limited scope of application which may not provide adequate protection for commercial data. One of the conditions for the application of the misappropriation doctrine is the existence of a competitive relationship between the commercial data controller and the user. No matter how the concept of a competitive relationship is expanded, to attract the application of the misappropriation doctrine, it is necessary that the controller and user of commercial data have at least some sort of connection. This means that the misappropriation doctrine may have difficulty constraining the use of commercial data by non-competitors. Moreover, the application of the misappropriation doctrine requires that the information protected be time-sensitive. Most commercial data requiring long-term protection, however, is not time-sensitive. This means that it is not possible for the misappropriation doctrine to provide protection for such commercial data.

Second, the misappropriation doctrine protects quasi-property without clearly specifying the content of the rights associated with that quasi-property. Therefore, the misappropriation doctrine may fail to draw the boundary between protected commercial data and freely available public domain resources. Furthermore, the misappropriation doctrine may not respond to the increasing demand for controllers to establish property rights over their commercial data in a growing digital economy. Moreover, the misappropriation doctrine may fail to fulfil the task of property rights deployment and benefit allotment.

Lastly, despite the existence of a substantial body of common law on the misappropriation doctrine, the criteria for its application remain ambiguous. As stated by Judge Posner, the misappropriation doctrine lacks clear boundaries, and the apparent precise five-factor test for its application may be illusory[27]. Whether the misappropriation doctrine can protect commercial data requires a case-by-case determination. It follows that a commercial data protection system based on the misappropriation doctrine may lack legal certainty. In this regard, it may be necessary to establish a legal system based on property rights to protect commercial data.

4. The way to a *sui generis* commercial data protection regimes

The discussion above suggests that existing IP regimes may not sufficiently protect commercial data. Therefore, it is necessary to develop a new approach to commercial data protection.

One alternative is to treat commercial data as a novel IP subject matter, on the basis of which a commercial data protection system may be established under the IP regime. This article disagrees with this approach, since: Firstly, commercial data differs from traditional IP subject matter in terms of features; Secondly, commercial data carries more complex interests; Finally, given that commercial data overlaps with some IP subject matters, the logical problem of categorization arises when commercial data is placed alongside works, trademarks and other subject matters.

This article favors establishing a *sui generis* system to protect commercial data, drawing on the rationale and normative design of the IP regime. This approach has several advantages. Firstly, it's beneficial for maintaining the stability and unity of the existing IP system and the integrity of its logical structure. Moreover, this approach can facilitate the design of systems tailored to the distinctive features of commercial data. This will help specify the legal nature of commercial data and the attribution of rights. Lastly, a parallel protection pattern between commercial data legislation and the traditional intellectual property system can highlight the status of data as an independent form of property.

Creating a commercial data protection system involves two main aspects. The first aspect is the creation of a novel property rights regime based on subject matter, exclusive rights, and duration of protection. This regime should correspond to the features of commercial data and is designed to protect

ISSN 2616-5783 Vol.7, Issue 2: 279-288, DOI: 10.25236/AJHSS.2024.070240

the interests of commercial data. The second aspect is the creation of a mechanism to strike a balance between protection and limitation of rights. This includes setting up exceptions such as fair dealing.

4.1. The creation of a novel property right

4.1.1. Subject matter

For commercial data to qualify as the subject matter of property rights, it must have the three nature of property: utility, scarcity, and availability[28]. Typically, this requires that the commercial data presents a potential or actual exclusivity. It also requires that producers have substantial investments in the commercial data set, and that the commercial data set has reached a significant quantitative level.

Commercial data is enormous in quantity and diverse in types. Since not all commercial data meet the requirements to be the subject matter of property rights, it is necessary to precisely identify the features of different types of commercial data and accordingly screen out those suitable for legal protection. In this way, the boundaries between private property and the public domain can be reasonably and clearly delineated. The following will analyse the subject matter of the right specifically based on the classification of commercial data.

Commercial data can be divided into scientific data, government data and company data based on the different application scenarios of the data. Among these data, company data may be eligible subject matter of commercial data property rights. By comparison, government data and scientific data in principle should not be private property due to the need for transparency and sharing.

Based on different degrees of publicity of the data, commercial data can be classified as public and non-public data. Discrete public data may be used by anyone as it is in the public domain. Accordingly, discrete public data may not be exclusively possessed, whereas a public data set may receive limited protection of property rights due to data set makers' investment. This is consistent with the practice of allowing third parties to legally collect or use publicly available data on a digital platform[26]. On the other hand, non-public data are generally under the control of a particular company or accessed by means of technical measures created by that company, which prevent others from grabbing the data. Non-public data, therefore, have *de facto* exclusivity and may be protected as property. In terms of the pattern of protection for non-public data, a patent-like method of protection is more advantageous than an absolute monopoly as with trade secrets, i.e., disclosure in exchange for monopoly for a limited period. In this way, the economic value of data can be realized and commercial data may flow and be shared more easily.

Depending on the degree of processing, commercial data can be classified as raw data and data products. Similar to public data, raw data can, in principle, be freely used by third parties, unless the raw data reaches such a quantitative scale that it acquires the nature of property. In contrast, data products are the subject matter of rights under the commercial data property regime. This is because data products involve substantial amounts of intellectual labour on the part of producers following extensive analysis, refinement, and integration, reflecting a high level of originality or creativity.

4.1.2. Duration

The duration of commercial data protection should not be too long. This is because commercial data is renewed rapidly. In a short period of time, commercial data may lose its original commercial value. In this regard, commercial data is similar to circuit layouts. Circuit layouts are protected under the IP regime for a shorter period of time than works under the copyright regime. A possible reason for this may be that circuit layouts may become obsolete in a relatively short period of time, thus reducing their commercial value. Given the dynamic feature of commercial data, a long protection period will not only fail to provide incentives, but will also increase the cost for users to access the data. In contrast, a shorter duration encourages commercial data to enter the public domain earlier. This may stimulate more innovation activities contributing to the data industry's prosperity.

4.1.3. Exclusive rights

To protect commercial data under a property regime, it is necessary to specify the particular rights enjoyed by commercial data holders, based on the distinctive features of commercial data. The design of these rights conferred on holders of commercial data has multi-level objectives: firstly, it is to protect the various interests carried by commercial data; secondly, it is to facilitate the sharing and transactions of commercial data based on the protection of those interests; lastly, it is to prevent the monopoly arising from property rights from slowing down the transmission and sharing of commercial

ISSN 2616-5783 Vol.7, Issue 2: 279-288, DOI: 10.25236/AJHSS.2024.070240

data in the markets and hindering the realization of the economic value of the data. Following is a description of both the positive and negative rights granted to commercial data holders.

Positive rights granted to commercial data holders include the right to use, license, and transfer. These rights facilitate the transmission and exploitation of commercial data on the market, thereby realizing the digital market's economic potential. Specifically, the right to use covers various commercial data exploitation, including mining, analyzing etc. On the basis of the right of use, the original right holder may allow other participants in the data industry to use commercial data by transferring and licensing their exclusive rights. This may reduce transaction negotiation costs and promote transparency and stability in the commercial data market.

In terms of negative rights, commercial data holders are entitled to prevent others from accessing and using commercial data without authorization. The exclusive right is not absolute; it is subject to exceptions and limitations. This ensures that certain parties are able to access relevant commercial data for specific personal or public purposes. In this way, the interests of various participants in the data industry (e.g. the general public, companies, users) can be balanced. Following are details about how the exceptions and limitations to the right to commercial data are formulated.

4.2. Mechanism for balancing interests in rights protection and limitation

The regime for protecting commercial data should not only provide exclusive rights to data holders, but also include mechanisms to limit the rights in order to balance the interests between protection and limitation. Through a mechanism for balancing interests, the commercial data protection regime can achieve a reasonable allocation of data resources, improve the efficiency of utilizing data resources, and enhance the role of commercial data as a driving factor for the development of the digital economy.

Specifically, the construction of the rights limitation mechanism consists of two main aspects.

The first aspect is to design the "fair dealing" exceptions for commercial data, drawing on fair dealing under the IP regime. Fair dealing is an important exception to copyright infringement, which usually refers to the use of works for specific purposes without the permission of copyright owners[29]. This exception is an important way of achieving a balance between the interests of copyright owners and the public.

In some countries and regions, "fair dealing" exceptions are reflected in their personal data protection legislation. These laws generally provide for consent of the subject of personal data as the lawful basis for data processing, while providing several exceptions. These exceptions can loosely be summarized as "fair dealing" with personal data. For example, Article 6 of the *GDPR* sets out five other circumstances where the processing of personal data is considered lawful in addition to data processing with consent, including data processing by controllers for the purpose of complying with a legal obligation[5]. Likewise, the Chinese Information security technology - Personal information security specification also provides exceptions to the collection of personal information with the consent of the subject, including the collection of personal data by academic organizations for statistical or academic research in the public interest[30]. Under the personal data protection regime, the 'fair dealing' with personal data can achieve a balance of interests between personal data subjects and data processors. This is instructive for the design of an interest balancing mechanism for commercial data.

For commercial data, fair dealing exceptions may apply to certain uses for specific purposes that do not adversely affect the legitimate interests of the data owner. For example, personal use of data for the purposes of learning and enjoyment, classroom presentations, and scientific research. Other examples include the expropriation, disclosure and provision of commercial data in the state and public interests, subject to certain conditions. These fair dealings exceptions are generally reasonable as they facilitate the sharing and exploitation of commercial data.

The second aspect is the establishment of commercial data sharing mechanisms. Theoretically, commercial data can support wider data sharing. Due to its non-rivalrous nature, commercial data can be used by participants in the data industry, including data owners, without compromising its quality. Aside from the data owner, other data processors may use commercial data to support or improve their products or services. Most commercial data owners do not have an incentive to restrict others' access to their data. This is because these uses of commercial data will not typically result in a loss of competitive advantage for the data owner, and they are not necessarily free of charge[31]. In this regard, the sharing of commercial data is permissible provided that it does not prejudice the interests of the

ISSN 2616-5783 Vol.7, Issue 2: 279-288, DOI: 10.25236/AJHSS.2024.070240

data holder, as it may provide third parties with the opportunity to benefit from the use of the data.

The FRAND principles in the standard essential patent licensing system may be introduced to commercial data sharing mechanisms. As suggested by the European Commission, access to anonymised personal data, which can be collected as commercial data, could be provided on a payment-based basis under the FRAND principles. Under the FRAND principles, where a patent is standard-essential, the patentee is usually required to provide a licence on fair, reasonable and non-discriminatory terms in order for the standard to be used as widely as possible. Similarly, third parties may request commercial data owners to provide data under the FRAND principles, usually on the basis of remuneration and subject to other specified conditions.

On the other hand, the establishment of a commercial data sharing mechanism based on the FRAND principles would face many problems. For example, how to set conditions for requesting access to commercial data? One approach is to make the unavailability of data from alternative sources, or the high cost of collection, a condition for third parties to request access to the data[32]. It appears that the criteria for determining whether this condition is met are ambiguous because what is data that is not available through other sources is unclear. Nevertheless, it is clear that this condition should not be too strict, considering that the purpose of accessing the data is to make it public and that such access is based on the payment of remuneration. Another question is how to determine a fair remuneration for data access? Considering that data are often a by-product, remuneration for access to commercial data should be different from the licence fee for intellectual property. In determining remuneration for access to commercial data, the basic principle is to enable companies to recoup the investment they have made in collecting the data, taking into account the characteristic that the data can be re-licensed and re-used repeatedly.

5. Conclusion

To overcome the deficiencies of the existing IP regime for protecting commercial data, it may be necessary to construct a *sui generis* property regime for commercial data. As a mature property regime, the IP system provides valuable experience for commercial data protection legislation. The IP regime can serve as a guide for the design of specific rules regarding the content of rights, the duration of protection, and the subject matter of the commercial data protection system. As a result of the parallel operation of the commercial data property system and the intellectual property system, better protection for commercial data can be provided, and circulation and utilization of commercial data can be encouraged.

References

[1] Ricketson S, Richardson M, Davison M. Intellectual property: cases, materials and commentary [M]. LexisNexis Butterworths, 2020.
[2] Mayer-Schönberger V, Cukier K. Big data: A revolution that will transform how we live, work, and think [M]. Houghton Mifflin Harcourt, 2013.
[3] Ministry of Justice. Unfair Competition Prevention Act (Japan) Act No 47 of 1993[EB/OL]. (1993-05-19). https://www.japaneselawtranslation.go.jp/en/laws/view/3629/en.
[4] Hongtao Nie. Mode exploration and system construction of enterprise data property protection[J]. Price: Theory & Practice, 2021(09):45-50.
[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 ('General Data Protection Regulation')[EB/OL]. (2016-04-27). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.
[6] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases[EB/OL]. (1996-03-11). https://eur-lex.europa.eu/ legal-content/ EN/TXT/? uri= celex%3A31996L0009.
[7] Copyright Act 1968 (Cth)[EB/OL]. (2022-07-01). https://www.legislation. gov.au/Details/ C2022 C00192.
[8] High Court of Australia. IceTV Pty Ltd v Nine Network Australia Pty Ltd [2009] HCA 14[EB/OL]. (2009-09-11). http://www6.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/HCA/2009/14.html.

ISSN 2616-5783 Vol.7, Issue 2: 279-288, DOI: 10.25236/AJHSS.2024.070240

[9] Xu Shi. An Intellectual Property Protection of Corporation's Data: Current Methods and Beyond[J]. Oriental Law, 2018(05):55-62.
[10] Supreme Court of The United States. Alice Corp. v CLS Bank Int'l, 573 US 208 (2014) [EB/OL]. (2014-06-19). https://supreme.justia.com/cases/federal/us/573/208/.
[11] National People's Congress. Patent Law of the People's Republic of China [EB/OL]. (2020-10-17). http://www.npc.gov.cn/npc/c30834/202011/82354d98e70947c09dbc5e4eeb78bdf3.shtml.
[12] Supreme Court of The United States. Mayo Collaborative Services v. Prometheus Laboratories, Inc., 566 US 66 (2012) [EB/OL]. (2012-03-20). https://supreme.justia.com/cases/federal/us/566/66/.
[13] Marrakesh Agreement Establishing the World Trade Organization, opened for signature 15 April 1994, 1867 UNTS 3 (entered into force 1 January 1995) annex Annex 1C ('Trade-Related Aspects of Intellectual Property Rights') Article 27[EB/OL]. (1995-01-01). https://www.wto.org/ english/docs_ e/legal_ e/trips_e.htm#art27.
[14] Mattioli M. Disclosing big data [J]. Minn L Rev, 2014, 99: 535.
[15]Agreement W T O. Marrakesh Agreement Establishing the World Trade Organization[J]. Multilateral Agreements on Trade in Goods, Annex A, 1994, 1.
[16] European Commission. Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)[EB/OL]. (2022-02-23). https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2022:68:FIN.
[17] Samuelson P. Information As Property: Do Ruckelshaus and Carpenter signal a changing direction in intellectual property law [J]. Cath UL Rev, 1988, 38: 365.
[18] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases[EB/OL]. (1996-03-11). https://eur-lex.europa.eu/legal-content/ EN/TXT/? uri= celex%3A31996L0009.
[19] Act on Copyright and Related Rights[EB/OL]. [2023-07-09). https://www.gesetze-im-internet.de/ englisch_urhg/englisch_urhg.pdf.
[20] Samuelson P. Mapping the digital public domain: Threats and opportunities [J]. Law & Contemp Probs, 2003, 66: 147.
[21] Stoll E. Hot News Misappropriation: More Than Nine Decades after INS v. AP, Still an Important Remedy for News Piracy [J]. U Cin L Rev, 2010, 79: 1239.
[22] Supreme Court of The United States. International News Service v Associated Press, 248 US 215 (1918) [EB/OL]. [2023-07-09). https://supreme.justia.com/cases/federal/us/248/215/.
[23] NBA v. Motorola, Inc., 105 F.3d 841 (2d Cir. 1997)[EB/OL]. [2023-07-09]. https://law.justia.com/ cases/federal/appellate-courts/F3/105/841/598844/.
[24] Facebook, Inc. v Connectu LLC, 489 F. Supp. 2d 1087 (N.D. Cal. 2007)[EB/OL]. (2007-05-21]. https://www.courtlistener.com/opinion/2415553/facebook-inc-v-connectu-llc/.
[25] Banxcorp v Costco Wholesale Corporation, 723 F. Supp. 2d 596 (S.D.N.Y. 2010). [EB/OL]. (2013-10-17). https://casetext.com/case/banxcorp-v-costco-wholesale-corp.
[26] hiQ Labs, Inc. v LinkedIn Corporation, No. 17-16783 (9th Cir. 2022).[EB/OL]. (2022-04-18). https://law.justia.com/cases/federal/appellate-courts/ca9/17-16783/17-16783-2022-04-18.html.
[27] Posner R A. Misappropriation: A Dirge [J]. Hous L Rev, 2003, 40: 621.
[28] Alchian A A. Some economics of property rights[J]. Il politico, 1965: 816-829.
[29] Australian Copyright Council. Fair Dealing: What Can I Use Without Permission [EB/OL]. (2020-01-01).https://www.copyright.org.au/browse/book/ACC-Fair-Dealing:-What-Can-I-Use- Without - Permission-INFO079.
[30] Standardization Administration of PRC. Information security technology - Personal information security specification [EB/OL]. (2020-03-06). http://c.gb688.cn/bzgk/gb/showGb? type=online&hcno =4568F276E0F8346EB0FBA097AA0CE05E.
[31] Mayer-Schonberger V, Ramge T. A big choice for big tech: share data or suffer the consequences [J]. Foreign Aff, 2018, 97: 48.
[32] Drexl J. Designing competitive markets for industrial data [J]. J Intell Prop Info Tech & Elec Com L, 2017, 8: 257.