University of New South Wales Law Research Series

TRADE IN PERSONAL DATA: EXTENDING INTERNATIONAL LEGAL MECHANISMS TO FACILITATE TRANSNATIONAL TRADE IN PERSONAL DATA?

LEON TRAKMAN, ROBERT WALTERS AND BRUNO ZELLER

(2020) (2) EDPL, 1
[2020] *UNSWLRS* 37

UNSW Law
UNSW Sydney NSW 2052 Australia

Trade in Personal Data: Extending International Legal Mechanisms to Facilitate Transnational Trade in Personal Data?

*Leon Trakman, Robert Walters, Bruno Zeller**

The transnational trade in personal data, while emerging as a valuable economic activity, poses many challenges for regulators and organizations. One of the major challenges is the fragmented and ad hoc approach taken by countries, and the European Union, in their data protection laws. This has led to data protection laws varying greatly from jurisdiction to jurisdiction. This paper will explore alternative legal mechanisms that might be available in the international arena to assist in the control and regulation of trade in personal data. The starting point is to review the use of different approaches that are adopted in intellectual property and copyright law to address this issue. Another vantage point is to espouse a contractual approach, which arguably is most achievable because the general principles governing contractual obligations are similar in most jurisdictions. This paper will argue that the Convention on the International Sale of Goods (CISG), can provide an alternative legal mechanism that can effectively help to regulate the cross-border trade in personal data. The paper will highlight how the CISG can be attractive as a practical legal mechanism for managing the sale of personal data through transnational contracts and by relying on copyright law. Applying the CISG provides individuals and entities with another legal mechanism that they can use effectively, not only to provide a level of control over personal data, but more importantly, to help facilitate trade in personal data. However, before concluding that the CISG is an effective legal mechanism, it will be important to determine whether personal data can be categorized as a good. It is our view that, in response to this challenge, personal data can be the subject of a sale of goods, and therefore can be subject to the application of the CISG.

I. Introduction

Back in 2017, *The Economist* published as story entitled, 'The world's most valuable resource is no longer oil, but data'. Since its publication, the topic has generated a great deal of discussion, and 'data is the new oil' has become a common refrain.[1] Kiran Bhageshur has highlighted an example where personal data and data generally will be combined and large quantities captured and aggregated to improve road congestion, lower Co2 emissions and make roads safer. Bhageshpur identifies autonomous vehicles (AVs) are evolving, and as the technology advances, these types of vehicles will increasingly be used around the world. The benefits are widely known: safer roads, a boost to the economy and less rush-hour traffic. How do we transition to a future where AVs become an established part of our lives? You guessed it: data. In this case, it requires hundreds of petabytes of data to form the data lake from which the AV self-

* Leon Trakman B. Com, LLB (Cape Town); LLM, SJD (Harvard). Professor of Law and Former Dean, Faculty of Law, University of New South Wales, Sydney; Robert Walters LLB (Victoria), MPPM (Monash), PhD Law (Victoria), Lecturer Victoria Law School, Victoria University, Melbourne, Adjunct Professor, European Faculty of Law, The New University, Slovenia, Europe. Bruno Zeller B. Com, B. Ed, Master of International Trade Law (Deakin), PhD (The University of Melbourne). Professor of Transnational Commercial Law, University of Western Australia.

1 Kiran Bhageshur, *Data Is The New Oil -- And That's A Good Thing, Forbes* Economist <https://www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/#3366ce2f7304> accessed 28 January 2020.

driving advanced machine learning solutions will come. It doesn't stop there. Each of these modern 'computing platforms that happen to be mobile' will generate terabytes of data per vehicle per week. Even assuming a 75% reduction in the number of vehicles on the roads, that amounts to many exabytes of data per year.[2] Moreover, Bhageshpur asserts that all of this is the data you keep.[3] Thus, at some point along the data supply chain there are likely to be contracts formed to manage the purchase and sale of that data. These contracts are unlikely to remain within national borders, but also to extend transnationally.

Despite attempts by some jurisdictions and international organisations to establish a baseline of concepts and principles to guide most data protection laws, the approaches to protecting personal data remain fragmentary and inconsistent in both law and policy. This is especially observable in the area of ownership, access to and trade in digital data, and, more specifically, in the commercial use of personal data. Corley noted that:

> With the newfound ease of collecting and transferring personal information,businesses have been able to collect, analyse, and package this sensitive data to sell to advertisers and other entities as a commodity.[4]

As information is collected in an ever more sophisticated environment a business needs, not only to understand its internal operations, but also how its competitors are reacting to changes in market demand in order to remain competitive. Hence, information is valuable as a commodity; and it is not surprising that companies specialize in harvesting and mining data (personal and commercial) in order to sell that data as a product to interested parties.

Simply put, it is undisputed that personal data is not only collected, but also sold and bought.[5] Data in general and personal data in particular has been recognised as a commercial asset. Interestingly, already in 1999 it was noted that the:

> Clinton Administration worked very hard to persuade Internet economy firms to adopt privacy policies and practices to make users more comfortable about engaging in ecommerce transactions in cyberspace, these efforts have done little to overcome the inertia of the current technical and economic environment that is generally hostile to privacy interests.[6]

Notwithstanding this criticism of inertia in protecting privacy in cyberspace, nothing fundamental has changed since this observation, with two exceptions. The one is wider recognition of the need to protect personal data. The other is that data subjects have been granted certain rights, such as the right to be forgotten in some jurisdictions. These exceptions are reflected in law, in realizing that 'individuals generally have a legal right to exclude other people from access to their private data, they may have a sense that they have an intellectual property right in the data as well as a legal right to restrict access to it.'[7]

This recognition of the need to protect personal privacy raises an important issue, namely, to determine which laws are applicable to achieve the desired effect of protecting personal data. A collateral issue is to establish how an aggrieved data subject can seek compensation for breaches of rights under an applicable data protection law.

All data protection laws regulate the protection of personal data of an individual (the data subject), but only in jurisdictions that have implemented these laws and hence that have defined what constitutes personal data.[8] In essence, the primary legal objective is to effectively prevent personal data from being exploited. Much has been written on this topic. However, there is a general market failure to regulate the interplay between the right to (intellectual) property and the right of access to regulatory intervention.[9] In other words, current day data protection laws have become an important tool to protect the privacy of individuals over the Internet. The prob-

2 ibid 1.

3 ibid 1; It's the new oil. If a vehicle accident occurs, you can call up the images recorded by the vehicles involved to decide what caused the accident and which AV algorithm needs improvements.

4 Morgan Corley, 'The Need for an International Convention on Data Privacy: Taking a Cue from the CISG' (2016) 41 Brooklyn Journal International Law, 722.

5 Simon Chesterman, *Data Protection Law in Singapore, Privacy and Sovereignty in an Interconnected World,* (Academic Publishing 2018) 1.

6 Pamela Samuelson, 'Privacy Intellectual Property?' (1999) 52 Stanford Law Review, 1125 - 1126.

7 ibid 1130.

8 Graham Greenleaf, 'Global Analysis of Data Privacy Laws and Bills Privacy' (2017) Law and Business International Report 145, 14–24.

9 Jacopo Ciani, 'Governing Data Trade in Intelligent Environments: Taxonomy of Possible Regulatory Regimes between Property and Access Rights' (2018) Intelligent Environments, 285 - 286.

lem - as with other regulations - is how data subjects can successfully claim that their personal data rights have been violated and secure compensation.

This paper will explore whether a transnational law could provide an effective legal framework in which to facilitate the international sale and transfer of personal data. Doing so, will identify another legal mechanism that, in part, can be used to protect personal data through transnational contracts. In proposing an international legal regime based on the Convention on the International Sale of Goods 1980 (CISG) to regulate the sale of personal data, the paper will argue that data, including personal data, is a good and not a service. Hence, a copyright can be attached to personal and other data which is tradeable and indeed, traded. It will discuss the legal ramifications for using the CISG to regulate the sale of goods that are subject to third party claims. The paper will also use a practical example to highlight the complexity in aligning personal data with transnational contracts. Therefore, it will examine personal data only, and not general data which is freely available and is not protected by data protection (personal) legislation.

II. Road Map

A central proposition of this paper is the CISG can be used to facilitate the trade in personal data. It can provide data subjects with an important, albeit limited, layer of control over personal data. The CISG also provides a legal mechanism by which data subjects can protect their personal data through contract, as well as intellectual property expressed through copyright. Put another way, once registered, that data is protected, but it can still be purchased and sold both within the nation state and across international borders.[10] Ciani has argued that 'what is crucial in order to realize this economic value is to ensure a possibility to make data available to third parties on the basis of a transfer or licence agreement.'[11] The main advantage of such an agreement is that, not only the owner of the data, but also the miner and end users can profit: hence, the value of data can be shared among all parties with a material interest in that data.

Steps in this direction have already commenced. The EU Commission's paper *Communication Building a European Data Economy*[12] 'considered the possibility of legislation on a data producer's right as a possible way to incentivise sharing data initiatives, enhance new business models for the exploitation of the data and unlock their economic value.'[13] However, once data is sold and bought, several questions arise. A threshold question is whether a sale of data is determined wholly by a series of contracts in which parties agree to buy and sell personal data. This reliance on a sequence of contracts for the sale of data is too simplistic. The problem is that, before any sale of data can take place, data needs to be harvested. However, that sale is subject to the data owner giving a right, in some jurisdictions, to the miner for the harvesting and use of the underlying data. The question then is whether the seller of that data has a right to sell it; and whether the buyer has any legal protection when he enters into a contract to purchase and use it? The issue is that data is an object that is subject to ownership first, and only on satisfying that requirement, can it be purchased and sold. In issue, therefore, are a further two decisive questions. Who has the right to sell personal data; and what is the basis for that right? The basis for the right is ownership of the object of that right, namely, the personal data itself. The problem is whether the law of property needs to be adapted to accommodate digital data as a legal object. Professor Van Erp aptly recognises this problem:

> The digital revolution, with its rapid growth of digital data and incredibly fast expansion of interconnectedness and interoperability, thus makes us question both what can be recognised as a legal object (can it include 'digital data' and if so, under which conditions?) and what the impact of the recognition of digital data as a legal object means for our understanding of ownership.[14]

The essential reality is that ownership needs to be redefined. Professor Sonnekus is correct, theoretically, in noting that 'it is 'tantamount to mental laziness' if

10 Simon Chesterman, 'After Privacy: The Rise of Facebook, the Fall of WikiLeaks, and Singapore's Personal Data Protection Act 2012' (2012) Singapore Journal of Legal Studies, 391- 415.

11 (n 9) 288.

12 COM (2017) 9 final.

13 (n 9) 288.

14 Sjef van Erp, 'Ownership of Data: The Numerus Clausus of Legal Objects'(2017) Brigham-Kanner Property Rights Conference Journal 6,235-236.

licence, copyright, and ownership are all seen as assets 'bundled under the same nomenclature as 'property.'[15] Yet, it is one thing to have that theoretical framework in place. It is another thing to be able to view the problem pragmatically in order to arrive at a practical solution, however temporary and piecemeal that solution may be. Commerce cannot wait until scholars have 'constructed' the ideal solution. This paper will therefore examine the pragmatic solution, rather than the scholarly one in redressing the questions posed above.

The following observations and viewpoints will guide the paper's analysis. First, it will examine that general information appearing on the net is public property. The assumption is that, like air, everybody is entitled to use it, without the need to purchase it first. One example of such general information traded generally over the Internet relates to the purchasing patterns of customers who shop at a particular outlet. However, this assumption is questionable, especially when the purchasing patterns of customers lead to invasive marketing to them. Furthermore, this first assumption will be outside the purview of this paper.

Second, the paper will evaluate the scope of 'protected information', namely, personal data that somebody owns. The concept of 'protected information' is reflected in the European Union's General Data Protection Regulation (GDPR) which the paper will assess. Third, the paper will consider whether 'personal data may be owned by data producers, controllers or processors, in the same way as non-personal data, but within the applicable limits imposed by the GDPR,'[16] and when the data subject voluntarily relinquishes ownership. Fourth, the paper will address the reality that digital assets have a commercial value, otherwise that data would not have been so conscientiously collected. Fifth, it will assert that the law protecting personal data, unfortunately, has not yet caught up with the reality: that digital assets are not physical assets, and that the law needs to be adapted to accommodate this deficiency. Importantly, the paper will contend that this adaptation of law to realism is necessary, even though courts in multiple jurisdictions recognise rights to monetary claims arising from contracts and also accept intellectual property rights. The reality is that '[c]ourts that understand all this clearly face a dilemma, but they do not know how to develop the laws to embrace the virtual reality.'[17] The obstacle underlying this judicial dilemma is that pure information cannot be protected easily, if at all. This judicial quandary is illustrated by an English case that responds to the obstacles, but fails to provide a clear answer. In *Your Response Ltd. v. Datateam Business Media*,[18] a data manager was engaged by a publisher to maintain a database. Once the contractual relationship was terminated, the manager asked for his fee. The publisher refused; and the manager, in turn, refused to hand over the database. There was no express term in the contract providing the publisher with access to the data. The court determined that:

> An electronic database consists of structured information. Although information may give rise to intellectual property rights, such as database right and copyright, the law has been reluctant to treat information itself as property. When information is created and recorded there are sharp distinctions between the information itself, the physical medium on which the information is recorded and the rights to which the information gives rise. Whilst the physical medium and the rights are treated as property, the information itself has never been.[19]

Simply put, the court held that control over a database is not the same as possession of a physical asset and that the control of *Your Response's* database did not fully exclude the publisher.[20] In essence, the court recognised that the information itself cannot be protected by law, but left open the issue over whether data could be so protected.

Section III will highlight the current debate over the property, contract and transnational approaches to protecting personal data. It will argue that a contractual approach, expressed through copyright law, is ordinarily most able to protect both the original owner, namely, the data subject, and the producers of databases, given that a sequential transfer of rights can be accomplished contractually. Section IV will set out which data in a commercial setting needs to

15 Jean Sonnekus, 'The Fundamental Differences in the Principles Governing Property Law and Succession from a South African Law Perspective' (2014) 3 European Property Law Journal 130, 136.

16 (n 14), 289.

17 ibid 246.

18 *Your Response Ltd. v. Datateam Business Media* [2014] EWCA (Civ) 281.

19 ibid, para 42.

20 (n 14) 245.

be protected; and highlights the complexity in aligning personal data with transnational contracts in relation to both data protection and its transfer. Section V will explain why copyright law provides a practical business-like solution to these issues, illustrated through the Convention on the CISG. It will challenge the incongruity that arose when 'the objects which result from human creativity ('intellectual property'), although accepted as legal objects, were classified as being outside traditional property law.'[21] It will also argue that the CISG, as a transnational legal mechanism,, is capable of protecting personal data through IP rights. Its effectiveness extends beyond providing another layer of legal control over personal data directed at protecting the privacy of data subjects. Its value is to facilitate an understanding of how personal data can be effectively protected through copyright law, while being transferred and traded on the international market.

III. Protection of Data

Currently the question of which legal mechanism protects data can be found in the data protection laws of nation states and the European Union (EU). However, under transnational contractual arrangements, there is little guidance on the level of protection these laws provide, even though the right to transfer personal data is recognised in discrete circumstances.

Nonetheless, several suggestions have been advanced to resolve the issue of breaches of data protection laws, namely, through the property [intellectual] approach and the contractual approach.[22] This paper will respond by arguing that the CISG endorses an alternative albeit limited option, in providing a level of control over personal data that is being traded internationally and across jurisdictions that have different data protection laws. The importance of this transnational alternative is the reality that the Internet does not recognise jurisdictional borders. Arguably, this transnational approach to data protection and its sale is preferable to diverse national laws that afford little certainty in safeguarding personal data.

Conversely, national laws can provide greater certainty in implementing the intellectual property or contractual approaches to data protection, even though there is little coalescence across legal systems and jurisdictions over the nature and construction of property and contractual rights. This lack of coalescence is ever more notable in relation to the ownership and sale of data whose transmission transnationally is difficult for states to regulate consistently under their domestic laws.

This paper will focus on how the CISG can be used to resolve the impasse across nation states over the scope of property and contractual rights over personal data. The test of time will determine whether this approach will prevail in multiple domestic jurisdictions or otherwise.

1. The Intellectual Property Law Approach

Property generally deals with the legal relationship between a subject 'vis-à-vis a considerable number of other subjects, regarding an object.'[23] Professor Van Erp appropriately notes that 'from the perspective of today's society, in which the virtual economy is almost becoming more important than the 'real' economy, the classical approach to property law must be revisited and re-evaluated for digital assets.'[24] In relation to property rights, Ciani contends:

> If the market works well in enabling transactions in other commodities, covered by property rights, it would presumably work for transactions in with first labour (Locke) or occupancy (Pufendorf), those who *first* collect the data, or data as well. Just like generate derivative data from a primary data sets are best entitled to keep their possession, because without them the data would not be existent in the IoT environments. Under this interpretation, all data seem to be explicable and justifiable as belonging to the data collectors because they ordinarily are the first to engage in such data collection.[25]

One of the discernible problems with this approach is that data must have an origin, as well as an answer

21 ibid 255.

22 Jacopo Ciani, 'A Competition Law Oriented Look at the Application of Data Protection and IP Law to the Internet of Things: Towards a Wider 'Holistic Approach', in M Bakhoum et al (Eds) *Personal Data in Competition, Consumer Protection and Intellectual Property Law* (Springer 2018).

23 (n 9) 241.

24 ibid.

25 (n 22).

to the question as to who owns the original personal data. Ciani does not fully answer this question. In addition, the notion that the property approach assumes the first collector of data is in the best position to keep the data[26] is overbroad. The approach is plausible only if the first collector was given assent to collect the data, distinguishing that collection from the theft of that data. This approach is also not readily adaptable transnationally, as many jurisdictions accept that 'physical' objects are capable of ownership but less so intangibles, such as in German law.[27] However, it must be recognised that the property right model offers two obvious benefits, as portrayed by Pamela Samuelson:

> First, it [the property right model] would establish a right in individuals to sell their personal data and thereby capture some of the value their data have in the marketplace. Second, a property rights model would force companies to internalize certain social costs of the widespread collection and use of personal data now borne by others.[28]

These advantages of the property right model must be weighed in light of the fact that it would 'in essence, establish a new form of intellectual property right in information. But it would be an intellectual property right of a very different sort than existing regimes provide.'[29] The real issue is that the law has not found a solution to overcome the disjuncture between personal property and pre-existing conceptions of property. A person's estate is comprised of all physical things and all patrimonial rights. However, a patrimonial right (eg, a right arising from a contract) cannot be owned. A person can only be 'entitled' to it, although entitlement in economic terms comes very close to ownership.[30]

It is the closeness between property and contract which gives rise to a preferable alternative, namely, a right modelled on an Intellectual Property Right [IP] and explicated through copyright and the right to trade secrets. The essence of that right, applied also to the right to privacy, 'is a relational entitlement to exclude specific actors from a resource, given a specific event, a given type of behaviour, and/or a given relationship between the actors'[31] Arguably, the essence of that right is grounded in existing IP laws that currently regulate information-based products. 'The economic rationale for intellectual property law arises from a public goods problem with information products that this law strives to overcome.'[32]

However, the fact that creative work has already been separated from general property law gives rise to an argument that property law is not the ideal vehicle by which to deal with the protection of personal data. The argument is all that much more justifiable at this time, given the diverse state of property law in different jurisdictions.

Trakman, Walters and Zeller argue that personal data should be considered as a property right.[33] They further assert that a central issue in so determining is whether data subjects need the protection of such rights in a technological revolution in which they are increasingly exposed to the use and abuse of their personal data. The authors also raise the further question of how IP law can provide data subjects with the requisite protection of their private space. They also consider whether other means of protecting personal data, such as through general contract rights, render IP protections redundant, or at least, less necessary.[34] The essence of their argument is that lawmakers often fail to distinguish between general property and IP protection of personal data; that IP protection encompasses important attributes of both property and contract law; and that laws that implement IP protection in light of its sui generis attributes are more fitting means of protecting personal data than the alternatives.[35] Moreover, they contend that, one of the benefits of providing IP rights in personal data goes some way to strengthening data subjects' control and protection of their personal data and strengthening data protection law more generally.[36]

However, affording personal data an intellectual property right is contentious. There is also a contradiction between the interplay between laws that provide for an intellectual property right and protecting

26 ibid.

27 ibid.

28 (n 6) 1126.

29 ibid 1126.

30 (n 14) 240.

31 Lauren Scholz, 'Privacy as Quasi-Property' (2016) Iowa Law Review 101, 1113.

32 (n 14).

33 Leon Trakman, Robert Walters, Bruno Zeller, 'Is Privacy and Personal Data Set to Become the New Intellectual Property?' (2019) International Review of Intellectual Property and Competition Law, 937-970.

34 ibid.

35 ibid.

36 ibid.

personal data. Yet, as there are increasing calls for a property right to be attached to personal data, the value of attaching such an IP right to a right in personal data cannot be ruled out in the future.

This futuristic case for a property right in personal data is accentuated by the ever growing 'cloud' in which sets of customer data are processed for commercial purposes that, in turn, are treated as trade secrets and *sui generis* database rights of cloud providers.[37] In the absence of any contractual provision, however, it is necessary to assess when and how to prevent a cloud provider from collecting its customers' data autonomously, namely, without the consent of the data subject. Francesco Banterle believes that both trade secrets and database rights should protect 'processed' data only.[38] The notion is that a database right protects data only after that data is collected. Indeed, the EU Database Directive aims to stimulate the development of processing systems, rather than the creation of data.[39] As a consequence, *sui generis* rights protect database contents as an organised set of rights.[40] This protection is broad and seeks to prevent any kind of extraction, even if indirect, which leads to the reconstitution of the database as a whole, or to substantial parts of it. It also applies to inhibit the re-utilisation of the extracted contents of that database in a different form, or in combination with different materials. Conversely, exceptions to such database protection are provided exclusively for scientific research, or for the extraction of substantial data from databases that are made available to the public (Articles 8 and 9 of the GDPR). Yet, these constraints do not provide full clarity over the boundaries of database rights. As Banterle highlights in light of Recital 45 of the GDPR, a database right does not constitute an extension of 'protection to mere facts or data'.[41] As the European Commission acknowledged, back in 2005, a ''*sui generis*' right comes precariously close to protecting basic information.'[42]

> Banterle goes onto to say that:
>
> Property in data challenges traditional concepts of civil law. Data are immaterial goods, which fall outside the classical scope of property. Conversely, ownership of immaterial assets has been traditionally identified in intellectual property. Yet information *per se* has a public good character and IP law tends to exclude the creation of property rights in it. As a confirmation, trade secrets (which may protect raw information) are rarely conceived as a property right. And even the database *sui generis* right is not designed to protect the creation of data. Furthermore, property rights in goods are subject to a *numerus clausus* principle, preventing operators from creating previously non-existing property rights. The same principle applies to intellectual property, where law must determine the relevant subject matter. Thus, interests in *res incorporales* not included in existing property rights benefit from a limited protection, which is characterised by the absence of exclusivity.[43]

In essence, data is not treated as property, nor ordinarily protected by an intellectual property right. The result is that non-corporeal rights, at best, enjoy limited legal protection. The next sub-section will analyse whether contract law offers a better solution to the facilitation of trade, dissemination and protection of data than attempts to protect data as property. It will propose that IP and copyright law in particular, when used in tandem, are able to encompass both contract and property rights in data, transcending the disparity between those rights.

2. The Contract Law Approach

The contractual approach arguably is the least complicated approach to the protection, trade and transfer of data, in part because general principles of consensual relationships between the contracting parties are similar in most jurisdictions. As Ciani remarks:

> It is generally accepted that freedom of contract should be 'king' in this area and this idea has been

37 Francesco Banterle, 'The Interface between Data Protection and IP law: The Case of Trade Secrets and Database Sui Generis Right in Marketing Operations, and the Ownership of Raw Data in Big Data Analysis'
in Bakhoum et al (eds) *Personal Data in Competition, Consumer Protection and Intellectual Property Law Towards a Holistic Approach?* (Springer 2016).

38 ibid.

39 Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77.

40 C-304/07 *Directmedia Publishing GmbH v Albert-Ludwigs-Universität Freiburg* CLI:EU:C:2008 [2008] 552.

41 ibid.

42 European Commission (2005), DG Internal Market and Services Working Paper: First evaluation of Directive 96/9/EC on the legal protection of databases, Brussels, 12 December 2005, Part. 5.2 <https://ec.europa.eu/info/sites/info/files/evaluation_report_legal_protection_databases_december_2005_en.pdf> accessed 26 May 2020.

43 (n 37).

> strengthened after the CJEU's 2015 decision in *Ryanair v PR Aviation*, according to which if a database is not protected by the database right, freedom of contract applies, subject to any restrictions imposed by competition laws or national laws.[44]

This doctrinal rationale is that freedom of contract serves as a pervasive right by which persons with rights to data can sell or otherwise transfer that data to others. In the absence of personal data being protected through data base rights, freedom to contract protects that data. That freedom to transact is denied, however, on grounds contracting in that data is illegal, anti-competitive, or otherwise public policy.

Samuelson provides a functional reason for protecting "information privacy'. One of the virtues of a contractual approach to protecting information privacy is that it can accommodate the multiple interests people have in personal information, the contextual nature of determinations about the appropriateness of collection or use of personal data, the significance of consent as a factor in determining appropriate uses, and the evolutionary nature of social understanding about information privacy. It is a flexible, adaptable, market-oriented way to allow individuals to control uses of personal data.[45]

The rationale, here, is that the law of contract can help to facilitate trade in personal data, while also in providing a level of privacy protection. This protection is achieved through contractual terms, providing that the owner of personal property and the commercial user are continuously and directly connected - contractually. Insofar as these connections are lacking, copyright law(s) can help to fill the gap by ensuring the protection and facilitation of trade in that personal data. This paper will argue that, in filling such gaps, copyright law serves as the primary driver. As such copyright both affirms and supplements the protection of personal data by contract.

3. Transnational Law Approach

A transnational law approach can aid in resolving debilitating divergences in the national laws governing transborder trade in personal data. As this paper argues, the contractual approach, coupled with copyright, is best suited to, providing a level of protection of personal data generally, and inferentially, in transnational trade as well. As such, the contract can protect the original owner, namely, the data subject and the producers of databases, and enable a sequential transfer of copyright downstream. As a result, copyright is not tied to property law; rather copyright becomes a term of the contract that is part of the governing contractual law. Copyright also transcends the continuing flaw of 'treat[ing] intellectual property as simply a species of real property rather than as a unique form of legal protection designed to deal with public goods problems.'[46] Over-categorized as an intellectual property, copyright here is more suitably conceived a right or expectation that attaches to the sale of goods; hence copyright is contract based. As it is contract based, copyright can provide a level of protection to a group of data, including the sale of personal data.

A practical impediment is how to ensure that copyright, based in contract, can protect transnational trade in personal date. In particular, how can the CISG protect personal data beyond the law of a signatory state? Conceived more broadly, can the CISG serve as a model by which personal data is protected through the coalescence of contract and intellectual property rights? Specifically, can that coalescence prevent "goods", including data, from being sold. Can they prevent such sale if the right to sell those goods is subject to third party claims, howsoever those rights are generated?

For the CISG to respond affirmatively to these questions, in facilitating the transfer, trade and protection of data, there is need to satisfy three fundamental criteria: 'simplicity, practicality, and clarity.'[47] These criteria are fundamental to applying the CISG to data transnationally, and encompasses:its capitalization on key timing, its automatic application to private parties who live in signatory states, its use of simple, clear, and practical language, and its creation of a gapfilling mechanism to deal with issues not explicitly covered by the convention that should nonetheless be governed by it.[48]

---

44 (n 9) 294.

45 (n 6) 1130.

46 Mark Lemley, 'Property, Intellectual Property, and Free Riding, Stanford Law School' (2004) Working Paper No 291 August, 1-2.

47 Morgan Corley, 'The Need for an International Convention on Data Privacy: Taking a Cue from the CISG' (2016) 41 Brook J Int'l L, 721.

48 ibid 767.

Conversely, in not being able to apply the CISG simply, practically and clearly, to data, overall the application falls short of the CISG's stipulated requirements. Therefore, and given the need to satisfy these requirements in applying the CISG to protect personal data, Part IV will discuss the capacity of the CISG to regulate the commercialisation of data from three perspectives. The first is whether and how personal data can receive contractual and copyright protection under the CISG. The second is how the CISG might serve as a legal mechanism for managing personal data in transnational contracts. The third is by adopting a practical example to dissect the interface between the creation and sale of personal data. The analysis will focus on protecting personal data, not general data that is freely available and not personal data that is protected by legislation or administrative regulation.

IV. Protecting Data in a Commercial Setting

The problem with protecting data in a commercial setting is that not all data attracts copyright protection.[49] As noted above, pure information will not receive legal protection. It is arguable that only personal data can attract copyright protection, conceivably extending to databases that contain commercial data that is capable of being protected by copyright. To highlight the complexity in aligning personal data with transnational commercial contracts, a practical example is provided below that will set discussion throughout the remainder of the paper.

Company A sells chemicals for weed control. It keeps a database of its customers, containing among other things: their personal name, date or birth and addresses, quantity of purchases and size of property. This information is collated in several international jurisdictions where Company A is simultaneously located. The database, with this identifying information, is owned by Company A that has an intellectual property right and/or copy right over the computer database.

Company B, the chemical manufacturer (also located in multiple international jurisdictions), approaches Company A and requests to purchase information in relation to the type of chemicals which are being sold in the relevant sector supplied by Company A. Company A sells the information to Company B, which not only contains the types of chemical products, but also the quantity bought by individuals and entities, including personal details/data. Company B uses the information supplied by Company A in a publication. It maintains that the biggest sellers in the region purchase chemical products which are environmentally friendly and which have, to date, not posed health hazards or damaged on local environmental amenities. It also discloses the personal details of customers of both Companies in different countries.

The material questions are several-fold. First, is the personal information provided by the farmer or chemical user to Company A, which is stored on Company A's database, protected by copyright? Secondly, did Company A have the right to sell the personal data, particularly transnationally? Is A's database itself protected by copyright? To answer these questions in order to determine the scope of Company A's copyright protection, it is necessary to examine domestic laws beyond laws that protect personal data. This resort to domestic law is necessary because the CISG does not define industrial property or intellectual property. In particular, Article 7 of the CISG provides that disputes over copyright protection is to be determined by the applicable domestic law.[50]

Therefore, it is useful to consider the application of the laws of Australia to the illustration above. The starting point is that, under Australian copyright law, facts and data are not directly protected by copyright. However, the collection of data, a dataset, or a database may be protected by copyright, provided that the data in issue is sufficiently original.[51] Whether something is sufficiently original to be protected by copyright depends on whether it has been produced

49 Instituut voor Informatierecht 'Privacy, Data Protection and Copyright: Their Interaction in the Context of Electronic Copyright Management Systems' (1998). Even though the report was referring to the former Directive 95/46/EC (OJ No L 281, 23.11.1995, 31), now replaced by the GDPR, the ambit of data protection laws is restricted to situations in which *personal* data are processed. In other words, the design and operation of an ECMS may be affected by data protection laws only insofar as the ECMS processes such data. The concept of personal data is usually defined by the laws in a broad and flexible manner.

50 United Nations Convention on Contracts for the International Sale of Goods, Article 7, <https://www.uncitral.org/pdf/english/texts/sales/cisg/V1056997-CISG-e-book.pdf> accessed 2 June 2020.

51 Anne Fitzgerald and Natasha Dwyer, 'Copyright in databases in Australia' <https://eprints.qut.edu.au/50425/4/50425.pdf> accessed 28 May 2020.

with independent intellectual effort. The operation of Australian copyright law in relation to databases is consistent with the *TRIPS Agreement* (Articles 9.2 and 10.2) and the *WIPO Copyright Treaty* (Articles 2 and 5). *TRIPS* require that copyright protection be extended to compilations of data or other material which, by reason of the selection or arrangement of their contents, constitute intellectual creations. A factual illustration is a literary work that provides intelligible information, as opposed to a random collection of data.[52] Furthermore, any computer program which underlies the database may also be protected by copyright as a literary work, separate from the contents of the database, because the definition of literary work includes a computer program or a compilation of computer programs.

The reasonable conclusion is that the database of Company A is protected by copyright. This conclusion is confirmed by case law in the United Kingdom. In *Flogas Britain Ltd.* v. *Calor Gas Ltd*[53] the plaintiff sought damages from the defendant for use of a database maintained by the plaintiff that contained information on its customers, their names, addresses, contact details, contract dates, pricing and other information. The High Court of England and Wales held that:

> the information such as the names and addresses of the customers was protected by a database right and transfer of all or a substantial part of the contents of the database to another medium by any means or in any form amounted to such extraction as to constitute infringement of a database right.[54]

The Australian Federal Court, in *Acohs Pty Ltd v Ucorp Pty Ltd,*[55] distinguished between the creation of the database and its use. Importantly, this case also illustrates the boundaries of an original work that is protected by copyright. Acohs claimed a copyright in the Material Safety Data Sheets (MSDSs) which it had prepared for companies that were obliged to make MSDSs available when supplying hazardous substances. Acohs maintained a database of information necessary to create MSDSs and a software system generated the MSDSs based on data entered by Acohs' employees or customers; that database was sometimes transcribed from existing MSDSs.[56] Upon a customer request for a particular MSDS, the system would call up elements from the database, compile the source code, and send the MSDS to the customer to view on-screen. The Federal Court held that:

> MSDSs written by Acohs' employees were original literary works as the author was required to select materials. However, MSDSs that were merely transcribed from existing MSDSs were not original because the transcribers did not make any original contribution and the system dictated the layout, presentation, and appearance of the MSDSs.

The Court of Appeal of England and Wales was required to delineate, definitively, the meaning and construction of personal data in *Coogan v News Group Newspapers Ltd & Anor.*[57] It ruled that confidential personal information is intellectual property under section 72 of the *Senior Courts Act 1981.*[58] The Court reviewed the construction of section 72 in the following terms:

> (1) In any proceedings to which this subsection applies a person shall not be excused, by reason that to do so would tend to expose that person to proceedings for a related offence: (a) from answering any question put to that person in the first mentioned proceedings; or (b) from complying with any order made in those proceedings.
> (2) Subsection (1) applies to the following civil proceedings in the High Court, namely: (a) proceedings for infringement of rights pertaining to any intellectual property or for passing off.[59]

Section 72 of the *Senior Courts Act* defines intellectual property as any patent, trademark, copyright, design right, registered design, technical or commercial information or other intellectual property.[60] The Court in *Coogan* went to some lengths to explain intellectual property and the meaning of commercial

52 *Hollinrake v Truswell 1894* [2].

53 *Flogas Britain Ltd.* v. *Calor Gas Ltd* [2013] EWHC 3060 (Ch).

54 ibid.

55 *Acohs Pty Ltd v Ucorp Pty Ltd* [2012] FCAFC 16; 201 FCR 173; 287 ALR 403; 95 IPR 1, 17 (2010) [7] and (2012) [8]. *Acohs Pty Ltd v Ucorp Pty Ltd* [2010] FCA 577.

56 ibid.

57 *Coogan v News Group Newspapers Ltd & Anor* [2012] EWCA Civ 48.

58 ibid, para 22.

59 ibid.

60 ibid.

information. It argued that the meaning of the expression 'technical or commercial information' has to be assessed by reference to the purpose of section 72, the immediate context of the expression, and the natural meaning of the words.[61]

The Court's most significant statement relating to intellectual property, however, lies in paragraph 38 of its decision. There, it attempted to provide a general definition *en passant*, stating that intellectual property protects information and ideas that have commercial value. The Court did caution that it would be dangerous to treat that proposition as a comprehensive definition; rather, it is a useful short and simple guide.[62] No case provides a clear and convincing definition of the data that is protected as intellectual property under the *Senior Courts Act 1981*, perhaps because the first attempt at a statutory definition of the protection of data appears to be in section 72(5) itself.[63]

The description of the information that is subject to legal protection, therefore, relates more to the purpose for which that data is being used, than its inherent nature. In issue is whether the 'information which[has] ...a confidential quality, relates to commerce,[64] and is of commercial value.'[65] As a result, if the purpose is to accord legal protection to personal data because that data is confidential and of commercial value, such protection could limit the scope of any agreement purporting to buy and sell that data.

Moreover, in applying UK and Australian law to the hypothetical problem above, the protection of copyright extends beyond Company A's data that includes the personal information of individuals that purchase the chemical products . The database itself is also protected if it contains original literature, rather than merely transcriptions. It is also clear that personal data that is treated as intellectual property in *Coogan v News Group Newspapers Ltd & Anor*[66] includes copyright law, among other conceptions of IP such as patent and trademark. It follows that the database of Company A is protected by copyright because it contains the personal data of individual farmers.

That copyright protection, in turn, is not limited to protecting personal data according to English and Australian domestic laws. The alleged breach of copyright is conceived, rather, as transnational in encompassing a sale of personal data across domestic boundaries. Discourse over the copyright protection of data, transnationally, is enlivened in evaluating the scope of articles 41 to 44 of the CISG, as are discussed below.

V. The CISG and Copyright

It is well known and understood that the CISG is not a code. The extent to which the CISG covers the contractual expectations of parties in relation to the sale of data needs to be explored. That exploration will serve as a starting point to discuss whether the CISG, or for that matter transnational law in general, such as under the UNIDROIT Principles, can resolve some of the problems that arise in protecting personal data in transnational contracts of sale.

1. Is the CISG Applicable?

Several preliminary questions need to be overcome before determining that the CISG is applicable. One question is whether the sale of data constitutes the sale of a good or a service under Article 3(2) of the CISG.[67] The answer proposed is that the mining of personal data constitutes a bringing together of goods and therefore does not constitute a service. Once that personal data is sold, the purchaser does not buy a service: he/she buys goods. Viewed appositionally, it is argued that the CISG ought not to apply if the preponderant part of the obligation of the seller consists of the supply of labour or other services. Reaching that determination depends on both

61 ibid.

62 ibid.

63 ibid, para 36-38.

64 ibid, para 23.

65 William Cornish W, David Llewelyn, Tanya Aplin, 'Intellectual property: patents, copyright, trademarks and allied rights' in Sweet and Maxwell (Eds) *Coogan v News Group Newspapers Ltd & Anor* [2012] EWCA Civ 48, 36-38.

66 [2012] EWCA Civ 48.

67 United Nations Convention on Contracts for the International Sale of Goods, Art 3(2) <https://www.uncitral.org/pdf/english/texts/sales/cisg/V1056997-CISG-e-book.pdf> accessed 30 May 2020; Art
3(1) Contracts for the supply of goods to be manufactured or pro duced are to be considered sales unless the party who orders the goods undertakes to supply a substantial part of the materials ne cessary for such manufacture or production. (2) This Convention does not apply to contracts in which the preponderant part of the obligations of the party who furnishes th e goods consists in the supply of labour or other services.

the purpose underlying the CISG, according to the purpose and the context in which it is applied. The purpose of the CISG is to regulate transnational, as distinct from domestic contracts of sale.[68] The word 'goods', in turn, depend on the situation in which it is applied. As the English Court of Appeal held in *The Noordam*: 'The word [goods] is of very general and quite indefinite import, and primarily derives its meaning from the context in which it is used.'[69]

Saidov and Green aptly note that 'the law should look to the context of each individual agreement, just as it does with other products, in order to identify the precise nature of the contract at issue, and to deal with it appropriately.'[70] Therefore, in order to strengthen the argument that data generated by computers is a good, it is helpful to apply the treatment that courts attribute to computer software by analogy to the CISG. Consider Hall J's remarks in *South Central Bell Telephone Co v Sidney J Barthelemy*:[71]

> The software itself, is the physical copy, it is not merely a right or an idea to be comprehended by the understanding. The purchaser of computer software neither desires nor receives mere knowledge, but rather receives a certain arrangement of matter that will make his or her computer perform a desired function. This arrangement of matter, physically recorded on some tangible medium, constitutes a corporeal body.[72]

In responding to Hall J's comments, Joseph Lookofsky argues that a sale under the CISG need not always entail the sale of a tangible thing.[73] He maintains further that the CISG could be applied to computer software and specifically, to diverse forms of software licensing. Lookofsky elaborates by proposing that the sale of goods, like software, frequently involves a mix of sales of goods and services:

> Though we cannot see or touch it, a computer program is not really all that different from a tractor or a micro-wave oven, in that a program—designed and built to process words, bill customers or play games—is also a kind of 'machine'. In other words, a computer program is a real and very functional thing; it is neither 'virtual reality' nor simply a bundle of (copyrighted) 'information.' Once we recognise the functional nature of a program, we begin to see that the CISG rules (on contract formation, obligations, remedies for breach etc.) are well-suited to regulate international sales of these particular 'things'.[74]

There is no conclusive evidence that the CISG must only ever apply to goods that are tangible. A German court remarked that: 'At the most, it is standard software that can be viewed as a movable object and therefore be considered to be 'goods' in the terms of the [CISG] Convention.'[75] In determining whether a 'scholarly market analysis' is a good, the court held that 'the sale of goods is characterized by the transfer of property in an object.'[76] In dismissing the claim, the court noted:

> In the present case, however, the right to utilize an intellectual product of work is in the foreground; the work is embodied in a written form solely to make it intellectually graspable, and the form of the embodiment is of secondary importance to the commissioner of the study.[77]

The problem in our view is that, with the advent of the Internet, this view that the writing form is solely to make the product intellectually graspable, is increasingly flawed. It presupposes that the Internet is no more than a means of recording and conveying information. This ignores how the interpretation of data generated over the Internet influences the interpretation of that data, including the purpose in generating that data for value. The focus, today, is less on sharing information in virtual space, than on capturing and transmitting personal data because it has commercial value and is tradable.

As a result, it is our view that the trade in personal data for profit constitutes the sale of a good, or more explicitly, as the sale of property embodied in

---

68 ibid, art 3.

69 *The Noordam (No.2)* [1920] A.C. 904 [908-909].

70 Sarah Green and Djakhongir Saidov, 'Software as Goods' (2007) Journal of Business Law, 161-181. <http://www.cisg.law.pace.edu/cisg/biblio/green-saidov.html> accessed 2 June 2020.

71 *South Central Bell Telephone Co v Sidney J Barthelemy,* 643 So. 2d [1240].

72 ibid 1246.

73 Joseph Lookosfky, 'In Dubio Pro Conventione? Some Thoughts about Opt-Outs' (2003) 13 Duke J Int & Comp L 258, 274-277. Lookosfky points out that the CISG is an elastic document and it ought not be stretched beyond its essential design.

74 ibid, 276.

75 Germany 26 August 1994 Appellate Court Köln (*Market study case*), <http://cisgw3.law.pace.edu/cases/940826g1.html> accessed 2 June 2020.

76 ibid.

77 ibid.

that good. The implication is that personal data, as defined under the EU and in national law, constitutes intellectual property and is subject to a propertied right in that data.

Attempts to distinguish between a property right in tangible goods as distinct from intangible objects ought not to be overstated. As Teija Poikela observes, a possible dispute over whether electricity is tangible (a quantum) or intangible (a wave) is avoided by not treating electricity as a good. However, she elaborates that the sale of gas is regulated by the CISG.[78] Therefore gas constitutes a good. This is an interesting point because an individual can rarely see, touch or feel gas, other than in its liquid form. It is our view that, not unlike gas, data cannot be touched or felt. But personal data can be seen once it is printed onto paper or becomes visible on a computer screen. As such personal data it is good, not only because it can be seen, but also because seeing it is the source of its commercial value.

Hiroo Sono presents the predominant view is that the CISG applies to online software.[79] That view advocates for equal treatment of software delivered on a disk and online. He asserts that, since the sale of a physical copy of standard software and online software transactions are contracts for the same purpose, the law should be blind to the mode of delivery. Sono maintains further that software supplied online is a transaction in 'information' *per se* and thus can only be a 'licence', whereas software supplied by physical copies can be a 'sale' or a 'licence'. We support the view, that software traded on a physical copy and those traded online should receive the same treatment. We do not agree that the CISG should apply to the sale of physical copies of data but not the sale of online information by "license".[80] We do not support other commentators, to whom Sono refers, who seem to suggest that, since information can be recorded on a tangible media, online software transactions are no different from transactions using physical copies.[81] This view not only confuses tangible media with intangible information. It also overlooks the most crucial point, that intangible information is transferred from one party to another in online transactions. That view is also doubtful in maintaining that intangible information is only 'copied', and therefore that no property (ownership) passes from the seller to the buyer. Should this view prevail, that property does not pass in transfers of intangible information, there appears to be no sustainable basis upon which to apply the CISG to that information.[82] If the application of the CISG is limited to the transfers of physical copies, there is no room for the CISG to apply to intangible information. Nor could that the transfer of that information be the subject of a sale of goods. Even when physical copies are involved, if the contract is one of license, then the CISG would not apply (Article 3(2) CISG). The result of this distinction between tangible information that can be sold as goods, and intangible information that cannot be sold as goods, is likely to unduly restrict the application of the CISG.

Sono notes that what must be considered here, therefore, are contracts for the supply of customized software in which the property (ownership) is transferred from one party to the other. The difference between customized software and standard software lies in the involvement of a 'service' to develop the software; and that this raises the possibility of excluding software based on Article 3.[83] Therefore, Sono asserts that only customized software that transfers physical copies should be governed by the CISG. In reaching this conclusion, he contends that reference should be made to Article 3(1) CISG which provides the criteria to decide when contracts for the supply of goods to be manufactured or produced, are excluded from the CISG, itself. Accordingly, if the buyer does not undertake to supply a substantial part of the materials necessary to develop the software, Article 3(1) CISG does not exclude the application of the CISG. Thus, the debate for Sono is whether the arrangements were under a licence or otherwise. Personal data that is traded as an aggregated set of data contained on software would not necessarily have anything to do with the licence of that software. It is the data that is being traded, not the software. Thus, the contracts would need to be clear and specific that

78 Teija Poikela, 'Conformity of Goods in the 1980 United Nations Convention of Contracts for the International Sale of Goods' (2003) Nordic Journal of Commercial Law.

79 Hiroo Sono, 'The Applicability and Non-Applicability of the CISG to Software Transactions' in Camilla et al (Eds) *Sharing International Commercial Law across National Boundaries: Festschrift for Albert H. Kritzer on the Occasion of his Eightieth Birthday* (Simmonds & Hill Publishing 2008) 512-526.

80 ibid.

81 ibid.

82 ibid.

83 ibid.

it is the data, and not the software, that is being traded or disseminated for the contract to be subject to regulation by the CISG.

As a result, custom software, internet downloads, and standard mass-market licences are all included within the scope of the CISG's, as are data networks.[84] Based on Lookofsky's argument, data would also fall within the confines of property.[85] The conclusion is that the CISG can be used to facilitate the trade, dissemination and, in part, provide a level of protection to personal data in relation to transnational contracts if the data is connected to or is part of a 'good'.

2. Intellectual Property

Articles 41 to 43 of the CISG directly address the issues of 'industrial property or any other intellectual property.'[86] However, no definition can be found within the CISG as to the nature and scope of intellectual property. It is left to domestic law to do so, as is explained above. The CISG addresses sellers, requiring that they must sell goods which are free from 'any claim of a third party based on industrial property or other intellectual property.'[87] The effect is that sellers at least, must take care that all their goods do not infringe any data protection laws that are specifically 'under the law of the State where the goods will be resold or otherwise used.'[88] Arguably, therefore, any sale of goods into an EU state would be subject to the broader requirements of the the General Data Protection Regulation.[89]

As discussed below, Article 43 of the CISG should be read in conjunction with Article 41 in order to demonstrate that the function of Article 42 is to limit the seller's strict liability. Article 41 provides that the seller must deliver goods that are free from any right or claim of a third party, unless the buyer agrees to take the goods subject to that right or claim. However, if that right or claim is based on industrial property or other intellectual property, the seller's obligation is governed by Article 42. Additionally, Article 42, requires that the seller must deliver goods that are free from any right or claim of a third party based on industrial property or other intellectual property, about which the seller was aware, or could not have been unaware, before entering the contract. This requirement is subject to proviso that the right or claim is based on industrial property or other intellectual property.[90] The conclusion, in reading these Articles together, is that the 'seller's lack of knowledge of the defect that is a third-party claim is irrelevant'.[91] Therefore, the CISG automatically triggers a potential Intellectual Property claim by the buyer.

Article 42 requires the seller to deliver goods free from any third-party claim based on the seller's responsiblility to ensure that a third party does not possess an intellectual property right in the goods. The relevant time at which the seller must make that determination is at the time of concluding the contract. The third-party claim must also be applicable in the country in which the goods are to be sold or used. In effect, the seller must indemnify the buyer should a third party decide to enforce his or her intellectual property rights. In issue is the clear statement in Article 42 that the goods must be free from third party rights or claims. If not, the seller is in breach of his contractual obligations. John Honnold in 1999 noted that the purpose of Article 42 is to protect the normal expectation of a buyer that he is not purchasing a lawsuit.[92] This observation is still as valid today as it was in 1999. The issue as to who bears the burden of proof today is reinforced by Honnold's assertion

84 ibid, 277.

85 (n 73).

86 Convention on the International Sale of Goods 1980, art 41.

87 Convention on the International Sale of Goods 1980, art 42.

88 Convention on the International Sale of Goods 1980, art 42(1)(a).

89 General Data Protection Regulation, Official Journal of the European Union, L 119/12, at Preamble 63, Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject. Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.

90 ibid, (a) under the law of the State where the goods will be resold or otherwise used, if it was contemplated by the parties at the time of the conclusion of the contract that the goods would be resold or otherwise used in that State; or (b) in any other case, under the law of the State where the buyer has his place of business. (2) The obligation of the seller under the preceding paragraph does not extend to cases where: (a) at the time of the conclusion of the contract the buyer knew or could not have been unaware of the right or claim; or (b) the right or claim results from the seller's compliance with technical drawings, designs, formulae or other such specifications furnished by the buyer.

91 John Honnold, *Uniform Law for International Sales under the 1980* United Nations Convention, 1999, (Kluwer) 295 <http://www.cisg.law.pace.edu/cisg/biblio/honnold.html< accessed 2 June 2020.

92 ibid, 265.

then. As an Austrian case[93] noted, 'the general burden of proof pursuant to the CISG was on the party that wanted to rely on a provision in its favour, unless reasons of equity would demand otherwise'.[94] This logical extension of the above argument – also noted in Article 42 – is explained by the French Court of Cassation. It stated that 'the trial judges found that the buyer could not, as a professional, have been unaware of the counterfeit; therefore, the buyer acted with knowledge of the property right invoked'.[95] Hence, Article 42(2)(a) states that the obligation of the seller does not in all circumstances extend to delivering goods free from any intellectual property right.

Intellectual property rights are territorial in nature. The reason for subjecting them to territorial jurisdiction is that extending the seller's obligation globally would constitute a disproportionate and unnecessary obligation.[96] Even so, this view is now changing as many data protection laws, like the one in the EU, are extraterritorial in nature.

The territorial jurisdiction of domestic and regional laws governing intellectual property rights does not suggest that the CISG has limited value. On the contrary, the basic legal position remains as before, namely, that the extraterritorial reach of the CISG is limited. Simply put, a seller must take note of any data protection law. The seller must also appreciate that, depending on where his buyer lives, the seller's liability might be wider than that prescribed by the CISG. The Austrian Supreme Court noted: [T]he seller merely has to guarantee a corresponding conformity in certain countries, but not on a worldwide level. It is primarily liable for any conflict with property rights under the law of the State in which (not: 'into which'!) it is being resold or in which it is supposed to be used, provided that the parties took this State into consideration at the time of the conclusion of the sales contract. The burden of proof in this respect is on the buyer.[97] Therefore, intellectual property rights are also different to any claims of that goods are non-conforming, pursuant to Article 35[98] of the CISG. That is in accordance with Article 35, requiring the seller to deliver goods that comply with the standards expressly or impliedly agreed upon.[99] Furthermore, the seller may have an obligation to deliver goods that comply with local standards that are: a) applicable at the place of use of the goods if, at the time of the conclusion of the contract, the seller knew or could not have been unaware of that place; and b) in any other case, applicable at the buyer's place of business. Thus, the need for the buyer to be aware of the localised standards is paramount in the development of the transnational contract.

3. Party Rights of Claims

Notwithstanding the above, and viewed this way, Article 42 mandates that the seller is not only responsible for claims for third party breaches of property rights; but is also responsible not to enable a third party to secure an intellectual property right over the goods. Should the seller fail to exercise such responsibilities, he must indemnify the buyer if the third party decides to enforce those IP rights. The corollary is that the seller of personal data must be reasonably aware that he is selling a product over which a third party has an IP data right or claim. In theory at least, this position is correct. However, as practical matter it is difficult for individual data subjects to determine that the data being sold pertains to them alone, or to a class of data subjects. This is because most, if not all, data transacted in this way will be aggregated with other data that could amount to thousands or hundreds of thousands of data. After all, companies that mine personal data often sell a summary of their findings in which individual data is 'packaged' with the data of others, and/or yet other data. This makes identification of individual data difficult but not impossible in make.

Yet, viewed this way, the converse can equally apply. That is, where there is a breach of a copyright

93 Austrian Supreme Court (*Oberster Gerichtshof*) 12 September 2006 [10 Ob 122/05x].

94 Pace <https://iicl.law.pace.edu/cisg/case/austria-ogh-oberster-gerichtshof-supreme-court-austrian-case-citations-do-not-generally-12> accessed 2 June 2020.

95 France 17 December 1996 Supreme Court (*Ceramique Culinaire v. Musgrave)*, <http://cisgw3.law.pace.edu/cases/961217f1.html> accessed 2 June 2020.

96 Ruth Janal, 'The Seller's Responsibility for Third Party Intellectual Property Rights under the Vienna Sales Convention' in Andersen and Schroeter (Eds) *Sharing International Commercial Law across National Boundaries* (Hill Publishing 2008), 206.

97 Austria, Oberster Gerichtshof 12 September 2006 <http://cisgw3.law.pace.edu/cases/060912a3.html> accessed 2 June 2020.

98 Convention on Contracts for the International Sale of Goods 2010, art 35.

99 CISG Advisory Council Opinion No 19 Standards and Conformity of the Goods under art 35 CISG, <https://www.cisgac.com/file/repository/CISG_Advisory_Council_Opinion_No_19d.pdf> accessed 12 June 2020.

that relates to the database itself, preserving the status of the intellectual property afforded to that database will be important. To achieve this, the data base needs to be an original contribution to satisfy the relevant copyright requirements. Therefore, it is our view that the CISG is well placed to protect the sale of goods that are subject to intellectual property rights. However, in practice, this is problematic, because of the challenges individual data subjects will face in proving that any IP had been breached.

VI. Conclusion

Trading in personal data is likely to increase and become an even greater part of the evolving digital economy. However, current data protection laws are fragmented and ad hoc. This could encourage companies that trade in digital information to identify other legal mechanisms to assist them in transacting in personal data, particularly in selling that data across national borders.

This paper has demonstrated that the protection of personal data, once it is harvested and traded, is currently in a state of flux. Global, regional and national law have simply not caught up with the new reality that trading in data is significantly more profitable in the ever-expanding virtual world of the Internet. Nor is the classical law of property capable of protecting personal data that is traded *enmasse* within our cybernetic cosmos. Van Erp put it succinctly when he noted:

> Next to the 'real' world, we now have the 'virtual' world, which is just as realistic as the physical world around us. This virtual world demands a rethinking of classical property law, particularly the numerus clauses of legal objects.[100]

This paper has shown that transnational law, centred on the CISG, is able to protect personal data from economic exploitation by resort to both contract and property including copyright. The protection of personal data through intellectual property rights in general is ineffective. Reliance on copyright as a sub-category of property is viable. That viability is further justified by the fact that IP law diverges across domestic jurisdictions, in contrast to trade in personal data that is global in nature. Nor can the protection of personal data in global trade wait for domestic or regional legislatures and courts, to provide the relevant guidance in applying property law to the sale and purchase of personal data internationally.

The Convention on the International Sale of Goods can help to redress domestic laws that regulate the sale of personal data inconsistently and sometimes ineffectively. It can regulate the sale, transfer, dissemination, and to a lesser extent the protection of personal data across signatory states, while also affirming the choice of law rules of those states. Specifically, the CISG automatically applies to contracts of sale that satisfy its requirements, so long as state signatories have not excluded the CISG from applying to contracts concluded within domestically, as permitted by Article 6 of the CISG.[101] Even then, the exclusion of the CISG is to be disregarded whenever it does not appear from the contract between parties across jurisdictions, from their mutual dealings, or from information they disclose before or on concluding their contract.[102] Importantly, as this article has argued, the CISG applies to contracts for the sale of personal data as "goods" that are owned, particularly through copyright as property. This appeal to the CISG is also compelling, given divergence across jurisdictions over propertied rights in personal data, and the CISG's applicability to trade in intangible goods that encompass personal data.

---

100 (n 14) 235-236.

101 Doutor Jorge Morais Carvalho, *The Concept of Lack of Conformity: From the CISG to the Proposal on Online Sale of Goods*, (Universidade Nova de Lisboa 2017).

102 ibid.