University of New South Wales Law Research Series

IS PRIVACY AND PERSONAL DATA SET TO BECOME THE NEW INTELLECTUAL PROPERTY?

LEON TRAKMAN, ROBERT WALTERS AND BRUNO ZELLER

(2019) *International Review of Intellectual Property and Competition Law*
[2019] *UNSWLRS* 70

UNSW Law
UNSW Sydney NSW 2052 Australia

E: unswlrs@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

Is Privacy and Personal Data Set to Become the New Intellectual Property?

Leon Trakman · Robert Walters · Bruno Zeller

Abstract A pressing concern today is whether the rationale underlying the protection of personal data is itself a meaningful foundation for according intellectual property (IP) rights in personal data to data subjects. In particular, are there particular technological attributes about the collection, use and processing of personal data on the Internet, and global access to that data, that provide a strong justification to extend IP rights to data subjects? 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. A further question is how IP law can provide them with the requisite protection of their private space, or whether other means of protecting personal data, such as through general contract rights, render IP protections redundant, or at least, less necessary. This paper maintains 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. The paper demonstrates that one of the benefits of providing IP rights in personal data goes some way to strengthening data

L. Trakman
LLM, SJD (Harvard); Professor of Law and Former Dean, Faculty of Law, University of New South Wales, Sydney, Australia
e-mail: l.trakman@unsw.edu.au

R. Walters
PhD Law (Victoria); Lecturer Victoria Law School, Victoria University, Melbourne, Adjunct Professor, European Faculty of Law, The New University, Ljubljana, Slovenia
e-mail: robert.walters2@live.vu.edu.au

B. Zeller
PhD (The University of Melbourne); Professor of Transnational Commercial Law, University of Western Australia, Crawley, Australia
e-mail: bruno.zeller@uwa.edu.au

subjects' control and protection over their personal data and strengthening data protection law more generally. It also argues for greater harmonization of IP law across jurisdictions to ensure that the protection of personal data becomes more coherent and internationally sustainable.

Keywords Data protection · Intellectual property · Personal data · Privacy

1 Introduction

This paper explores the idea of personal data as the new intellectual property (IP). It emphasizes that IP rights over personal data are distinguishable from general property rights. More importantly, this paper argues that characterizing personal data that is protected by data protection law as IP provides data subjects with a higher level of protection of their personal data. The benefit of doing so, in our view, is in responding effectively to the need for data protection in the face of constant and unpredictable changes in current and future technology in which it is often not known if and how personal data will be protected. In other words, even with recent heightened understanding by the general community of the value and importance of protecting personal data over the Internet, it is still likely that future technology will do more to facilitate abuse rather than protecting personal data. This likelihood is already evident in the current regulatory framework that regulates trading in personal data, but not the manufacturer of the infrastructure, platforms and system that facilitate that trade. Therefore, it is argued that providing an additional layer of control over personal data may fill gaps in the regulatory framework. The view that a data subject should have control over their personal data has also been reinforced by Tim Berners-Lee, the alleged inventor of the World Wide Web who states that "You should have complete control of your data. It's not oil. It's not a commodity. You should not be able to sell it for money because it's a right"[1] For Berners-Lee, the current systems, platforms and infrastructure along with government regulation are far from achieving this.

In arguing for the protection of data as intellectual property, this paper makes a distinction between personal data as property, and personal data as IP. Furthermore, treating personal data as IP rather than general property, the paper highlights that general property rights overly rigidify the protection of personal data. However, it does recognize scholarly support for a general property right in personal data, a view from which this paper diverges. The paper also contends that protecting personal data as IP provides data subjects with protection against the misuse of their personal data by downstream (third-party) users with whom a subject does not have a contractual relationship.

Focusing on limitations in the legal protection of personal data, the paper examines how laws in the EU, Australia and Singapore, regulate the misuse of personal data, including through IP rights. It argues that such protections ordinarily benefit data subjects only indirectly, rather than provide them with a direct right of

[1] Berners-Lee (2019).

action against those who misuse or abuse their personal information. This is accentuated by the distinction that lawmakers often draw between sensitive data that is more stringently protected than general data, which is often not protected. In our view, insofar as regulators have placed a higher threshold on protecting a data subject's sensitive personal data, they have reinforced the benefit of according that subject, at the minimum, some level of IP protection. Nevertheless, it is our view that both general and sensitive personal data ought to be protected through IP rights.

The paper proposes how the current definition of personal data, the concept of consent (including consent for children), the right to data portability, and the right to access personal data in national and supranational laws can support IP rights in personal data. It maintains that, in *not* recognizing that IP rights include elements of both property and contract in personal data, the right to control the use of personal data dilutes the legal framework created by the EU, Australia and Singapore to regulate personal data. In addressing these issues, the paper identifies how IP measures can be further enhanced to strengthen the control of data subjects over their personal data, while not wholly discouraging the purchase and sale of that data by third parties.

In seeking these ends, the paper underscores that the protection of the personal information of data subjects through IP is an emerging and complex issue upon which there are divergent views that need to be reconciled. Two principle means of addressing this concern is through contract and property law.[2] More particular is the protection provided by IP law as a distinct *genus* of law that encompassed elements of both property and contract. This paper examines how the IP protection of personal data can be further emboldened by appreciating that IP is "[not] simply [as] a species of real property" but "a unique form of legal protection"[3] designed to defend rights or expectations that are attached to the sale of personal data over the Internet. As such, IP rights in personal data is appropriately protected as a "public good", as distinct from a general property right in that data.[4] What an IP right therefore accords the data subject is control over that data, for the purpose of retaining, using or selling it to data users with whom that subject does not have a direct contractual relationships. By these means, IP rights in personal data, including through the law of copyright and licensing agreements, are differentiated from general property rights that are identified with strict ownership of that data.

The paper does refer to IP as the ownership of personal data, consistent with scholarship using the term "ownership". However, it stresses that an IP right is more proximate to control than ownership of personal data, particularly in relation to third-party data users with whom the data subject lacks privity of contract. As such, that IP right is distinguished from a contract right that does not bind downstream data collectors, processors and users against whom the data subject often lacks the protection of enforceable contract rights.

[2] Zittrain (2000), p. 1203. Zittrain discusses how the music industry moved from being vulnerable to developing technological systems that could protect the IP of those that make music.

[3] Lemley (2004), pp. 1–2.

[4] *Ibid.*

This scoping paper also reflects on viable transnational solutions to data protection. A central focus is therefore on critically examining leading theories on the protection of data. Throughout the paper the argument will be made that intellectual property rights are a superior solution to other suggested mechanisms for protecting personal data.

To limit complications in the use of terminology, the paper gives the same meaning to personal data and personal information, as defined by the EU and embodied in the national laws of Australia and Singapore.

Finally, the paper examines how data protection laws redress the impact of ever-growing technologies that provide ever-widening sectors of society with access to sensitive personal data, notably to the data of vulnerable sectors of society, such as children. It proposes that the Internet's supporting infrastructure requires a global response to data protection of sensitive and other personal data, through the harmonization of laws. It evaluates recent case law that has afforded greater protection to personal data, including through IP rights. It also underscores the challenging social, economic and human rights issues that are faced by policy makers, legislatures and courts in regulating, effectively and also realistically, the use of new technologies that impact on virtually all who inhabit our global village.

Section 2 of the paper considers the significance of a right to privacy and the rationale for protecting personal data as intellectual property. Sections 2.1.1 and 2.1.2 identify the competing economic and human rights rationales for regulating the collection and use of personal data. Section 2.1.3 provides a brief outline of current technologies used to protect people's privacy online. Section 2.1.4 discusses the definition of personal data within the laws of the EU, Australia and Singapore, while Sect. 2.1.5 discusses that definition in relation to personal privacy. Section 2.1.6 highlights the distinction between the concept of consent to the use of personal data and an IP right that extends beyond that consent. Section 3 demonstrates how emerging case law in the United Kingdom and historical case law in the United States, have given rise to IP rights in personal data. Section 4 demonstrates the benefit of characterizing personal data as having an IP right, so that, as technology advances, data subjects will have greater comfort in having their personal data subject to graduations of legal protection. Section 5 concludes by highlighting key obstacles in protecting personal data and the value of IP in addressing those obstacles.

2 The Significance of a Right to Privacy

It is arguable that data subjects have privacy rights in their personal data and by extension, that they have IP rights in that data as well. The further postulation is that their IP rights extend beyond their privacy rights in the original data.

The intricate relationship between personal data and privacy is an important source of new thought. The rationale is that the introduction of data protection law has significantly promoted the protection of an individual's personal data, and subsequently the right to privacy over the Internet. In effect, the right to privacy

over the Internet is construed as a by-product of data protection law that has evolved to regulate the collection and use (trade) of personal data.

However, the understanding and acceptance of the right to privacy differs greatly amongst countries and regions of the world. Privacy itself has been influenced by culture, regional and global events. As such, it is largely a Western concept that has evolved in response to mass violations of personal security that occurred during World War II.[5] Subsequently, privacy emerged as a right in international public law, as explicated in the 1948 Declaration of Human Rights[6] and the United Nations International Convention on Civil and Political Rights 1966.[7] In 1980, the Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data was introduced.[8] Its purpose was to prevent violations of fundamental human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data, and the abuse or unauthorized disclosure of such data.[9] Privacy protections have evolved further in the new world. American judges and scholars, Warren and Brandis, defined privacy as the right to be let alone.[10] They also maintain that this right to privacy was already part of common law. They insist that, protecting one's home as one's castle, albeit subject to political, social and economic change, made it important to recognize that the protection of the right to be let alone is a legitimate extension of the right to privacy.[11]

The law of privacy has also evolved across the European Union (EU). Privacy emerged as a fundamental right in 1950, with the introduction of the European Convention on Human Rights (ECHR), ratified in 1953.[12] That Convention contains a right to a private life, although it does not specifically mention data protection.[13] This early right of a person to enjoy a private life was further strengthened by the EU Charter of Fundamental Rights 2000 which protects European citizens' private lives and also includes the protection of their personal data.[14] That Charter was, notably, the first legal document to include data protection as a fundamental human right, and binding on all Member States.[15]

[5] The Universal Declaration of Human Rights, adopted by the General Assembly of the United Nations on 10 December 1948 (General Assembly resolution 217 A) was the first collective response by member states on the fundamental and inalienable nature of human rights.

[6] *Ibid*.

[7] Adopted and opened for signature, ratification and accession by General Assembly Resolution 2200A (XXI) of 16 December 1966, entry into force 23 March 1976.

[8] Organization for Economic Cooperation and Development Guidelines governing the protection of privacy and trans-border flows of personal data (as amended on 11 July 2013), http://www.oecd.org/sti/ieconomy/privacy.htm.

[9] *Ibid*.

[10] Warren and Brandeis (1890).

[11] *Ibid*.

[12] Convention for the Protection of Human Rights and Fundamental Freedoms, 1950. Rome, 4.XI.1950, European Treaty Series – No. 5.

[13] *Ibid*, Art. 6.

[14] Articles 7 and 8, Charter of Fundamental Rights of the European Union, Official Journal of the European Union, 2000/C 364/01.

[15] *Ibid*, Art. 8.

The EU has, noticeably, placed human rights at the forefront of both law and policy, across virtually all sectors of society. European courts, following the EU's lead, have embodied this affirmation of human rights in their decisions. In *Nold Kohlen- und Baustoffgroßhandlung*[16] the court asserted its strong commitment to human rights. It ruled that, in safeguarding human rights, European courts were bound to adhere to constitutional traditions common to Member States. The Court therefore upheld measures to redress human rights abuses that it considered as being incompatible with fundamental rights as endorsed in the constitutions of those States.[17]

The right to the protection of property was also enshrined in Art. 1 of the First Protocol to the ECHR, as well as in Art. 17(1) of the EU Charter.[18] The 2008 Spanish case of *Productores de Música de España (Promusicae)*[19] was concerned with the refusal of a Spanish Internet (access) provider, Telefónica, to disclose to Promusicae, a music producer and publisher of musical and audio-visual recordings. The case was also concerned with personal data of certain persons to whom it had provided access to certain Internet services. Promusicae sought the disclosure of that information for the purpose of initiating civil proceedings against those persons. The court highlighted the need to reconcile the required protection of fundamental rights, specifically, the right to respect one's private life and the right to the protection of one's IP.[20] This decision paved the way to introducing the concept that personal data does not only contribute to the protection of privacy; it also gives rise to an implied legal relationship between personal data and IP within the EU Charter. It also gives balance to the trade in personal data, to which the laws aim, to varying degrees.

Australia, on the other hand, is still grappling with the concept of privacy in common law, particularly privacy over the Internet. The privacy laws of Australia have been in place for more than 30 years, with the Privacy Act being implemented in 1988. Even though these laws are not as mature as the EU's legal

[16] Case 4/73J *Nold Kohlen- und Baustoffgroßhandlung v. Commission of the European Communities.*

[17] *Ibid.*

[18] Official Journal of the European Communities C 364/1, Art. 17, "Right to property – 1. Everyone has the right to own, use, dispose of and bequeath his or her lawfully acquired possessions. No one may be deprived of his or her possessions, except in the public interest and in the cases and under the conditions provided for by law, subject to fair compensation being paid in good time for their loss. The use of property may be regulated by law in so far as is necessary for the general interest. 2. Intellectual property shall be protected."

[19] Case 275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU* [GC], 29 January 2008.

[20] *Ibid.* paras. 62–68. The Spanish court referred the issue to the Court of Justice of the European Union (CJEU), asking whether such personal data must be communicated, under community law, in the context of civil proceedings, to ensure the effective protection of copyright. It referred to Directives 2000/31, 2001/29 and 2004/48, read also in light of Arts. 17 and 47 of the Charter. The CJEU concluded that these three directives, as well as the e-Privacy Directive (Directive 2002/58), did not preclude Member States from imposing an obligation to disclose personal data in the context of civil proceedings to ensure effective copyright protection. The court concluded that "the Member States must, when transposing the directives mentioned above, take care to rely on an interpretation of those directives which allows a fair balance to be struck between the various fundamental rights … or with the other general principles of Community law, such as the principle of proportionality".

framework for data protection, they have established a structure for the protection of personal information (data). In taking a common law approach, Australian courts have applied the law of contract to determine the extent to which a right to privacy has been breached. They have done so notably by applying the law of equity to a breach of confidence, but they have not extended the law of torts to breaches of privacy over the Internet.[21]

The development of law in Singapore has been quite dissimilar to that in Australia and the EU. However, privacy in Singapore, in particular, has been shaped differently to the EU and Australia. This difference was expressed by the founding father of modern-day Singapore, the late former Prime Minister, Lee Kuan Yew who stated:

> I am often accused of interfering in the lives of citizens… Had I not done that we wouldn't be here today. And I say without the slightest remorse that we wouldn't be here, we would not have made economic progress if we had not intervened on personal matters – who your neighbor is, how you live, the noise you make, how you spit or the language you use.[22]

It is arguable from this statement that the general policy of protecting the right to privacy is antithetical to the Singapore's modernized political and economic ideology propagated by Lee Kuan Yew. In contrast, Simon Chesterman notes that many jurisdictions throughout Asia now embrace data protection law, even in the absence of any formal right to privacy.[23] Given the development of privacy rights in Asia and elsewhere, an important question, then, is how privacy rights in personal information can be extended to intellectual property rights in that information. In particular, if an individual has the right to privacy in respect of personal data, when and how can that right be supplemented by an IP right, and what is the value of recognizing that IP right?

2.1 Rationales for Protecting Personal Data

An important question is whether there is a strong practical and legally supportable justification for granting IP rights to data subjects in an era in which manipulation of data over the Internet is increasing and at a worrisome rate.[24] The first functional question is how such IP can provide meaningful rights to data subjects. The second question is how IP can provide better protection than alternative measures, such as through the law of privacy or consent to contract, either of which could conceivably render a property right in personal data unnecessary. A third question is whether the grant of an IP right to data subjects would undermine both freedom of expression in the use of that data, and the free trade in that data for commercial and public interest purposes.

---

[21] *See Doe v. Yahoo!7 Pty Ltd [2013] QDC 181.*

[22] Chesterman (2018).

[23] Chesterman (2012). Comparing these jurisdictions *inter se* poses another layer complexity because of the potential clash between the common law system of Australia and Singapore, and other Asian states whose legal systems are based on European civil law.

[24] On such abuse of the Internet, *see e.g.* Dhanjani (2015); Kozyris (2007).

If the case for granting IP rights in personal data is justified, the challenge is to balance the human rights protection accorded to data subjects with the economic right of data collectors and processors to trade freely in that data. If these alternative rights are recognized, the enduring issue is to determine how they ought to be balanced, such as through statutory requirements, or through the data subject's contractual, privacy, or tort rights in private law.

A further policy consideration is to acknowledge that, while individual states or associations of states such as in the EU, can protect personal data domestically, it is difficult for a multiplicity of states with different economic, social and political agendas to regulate personal data similarly. It is also challenging for them to address the constantly changing internationalization of the Internet and its infrastructure. On the one hand, nation states have not kept pace with global technological developments. Concentrating primarily on their distinct sovereign needs, they have engaged in ad hoc and inconsistent approaches to protecting personal data.[25] On the other hand, the development of data protection concepts and principles by the OECD and the EU has set benchmarks in data protection and has drawn other countries into their legal framework. The differential treatment of personal data by states has nevertheless led to ongoing tensions between legal convergence and divergence among states, including in harmonization of data protection laws. The lack of awareness and understanding by the general population as to how their personal data is being used, poses further difficulties for policy makers. Their challenge is to promote legal harmonization in protecting personal data that is comprehensible to the average data subject, transparent in its nature and operation, and capable of effective regulation.

The discussion below considers competing rationales for extending, or denying, IP rights to data subjects in their personal information. The ensuing purpose is to evaluate the potential for reconciling such differences, and to include IP protections within that reconciliatory process.

2.1.1 Economic Rationale for the Commercialization of Personal Data

On a general level, Merges, Menell, Lemley and Jorde argue that the economic rationale for protecting IP arises from the public interest in regulating markets in information-based products, giving rise to laws that regulate IP.[26] The economic rationale behind IP law therefore is to overcome the misuse and abuse of personal information.[27] Those authors add that, in the absence of IP rights, there may be little incentive to induce an optimal level of private investments in the production and dissemination of intellectual products.[28] The rationale is that the public at large benefits from such investments being made, regardless of whether those investments are in technology, artistic or literary fields.[29] However, today the Internet and supporting software and infrastructure provides an opportunity for organizations to

[25] *See* further Sect. 2.1.4.

[26] Merges et al. (1997), pp. 11–20.

[27] *Ibid.*

[28] *Ibid.*

[29] *Ibid.*

trade profitably in personal data and information. Therefore, even a minimal IP right in personal data creates at least some expectation that the data subject has another level of control over the commercialization and tradability of that data – outside of the current data protection laws.

The position taken by Merges, Menell, Lemley and Jorde, provides a solid foundation for arguing that personal data should be afforded an IP right. As they note, trade in personal data is no different to the trade (that has been occurring for decades) in commercial data that has also been provided IP protection. Furthermore, the right to privacy and hence protection is embedded in data protection laws. However, IP laws, arguably, would extend current data protection laws, as they attach a right to the owner of the data. Simply put, data protection laws not only protect the tradability of data, they also play a role in facilitating that trade. Hence, the dilemma is to reconcile the use of personal data as a tradable commodity in a market that attaches a commercial value to the data. This has led to conflicting scholarly views on how to resolve this dilemma, including through IP rights.

Taking a critical stance, Julie Cohen challenges the central proposition that, recognizing that IP rights in personally-identified data leads to more, not less trade, but produces less, not more, privacy.[30] However, Mark Lemley takes a conservative approach. He warns that, from a privacy perspective, IP is regularly signed away. Importantly, he expresses concern that the information revolution may reduce the protection that individuals ought to have over their personal data.[31] Lemley's view is espoused, in part, by Omer Tene and Jules Polonetsky. They argue that personal information should be regarded as neither an exclusive asset of individuals (the treatment of which may impinge on business trade secrets and IP rights), nor as exclusively the property of businesses that exclude individuals from benefiting from that property.[32] Tene and Poloentsky reject both propositions, arguing instead that personal information should be treated as a valuable joint resource and a basis for value creation and innovation. Their position therefore contests the notion that an IP right can be extended to personal data.

The emerging argument of whether a person has an IP right in personal data has also been recently summarized by Gianclaudio Malgieri. He contends that personal data and information have intrinsic value and therefore are eligible for protection as IP rights.[33] However, Malgieri points out that the intersection between personal data and IP is blurred.[34]

Despite the diverse views about whether personal data can, or should, be protected as an IP right, personal data is the subject of *sui generis* regulation. This

[30] Cohen (2000), pp. 1423–28.

[31] Lemley (2000). This view diverges from Lemley's earlier work, referred to in his article ibid in this note.

[32] Tene and Polonetsky (2013), p. 239.

[33] Malgieri (2018), pp. 118–140.

[34] *Ibid*.

includes the assertion that limits be placed on the propertization of personal data.[35] In particular, when the protection of personal data is in the public interest, such as for national security or law enforcement purposes, propertization of that data may be legally limited. Schwartz argues that specific regulation is needed to control the commodification of information, even personal information, in recognition of the additional uses and prospective transfers of personal data.[36] In effect, by implication he rejects that IP protection is the solution.

Schwartz maintains further that regulations directed at redressing the commodification of personal data place pressure on the better-informed party, to disclose material information about how personal data will be used.[37] His rationale is that this will render data subjects better informed of how their data and information will be used, as well as the purpose of that use. This creates an opt-in or opt-out process whereby data subjects have a choice to allow their data to be used, or to opt out of its use. This third element of Schwartz's argument, therefore, encompasses the principle of consent, namely, that data subject's consent to the collection and use of their personal data, as defined by the applicable law.

Schwartz argues, further, that under a consent-based model of decentralization, regulatory commissions should be established to oversee compliance with decentralized laws that regulate the collection and use of personal data.[38] What Schwartz advocates is evident in current legal frameworks in the EU, Australia and Singapore that have established Commissions, Commissioners and/or dedicated Agencies to assist in the regulation and implementation of data protection law. The EU has adopted a multi-layered regulatory approach that interacts with the national authorities of Member States. The creation of these regulatory bodies demonstrates that, while a consent-based model has value in regulating the use of personal information, a self-regulating model should be scrutinized by the agencies responsible for overseeing such market-based uses and abuses of personal data.[39] Implicitly, self-regulation by data collectors, controllers and users is only truly effective when they are subject to pre-set regulatory requirements that are enforceable *ex post* should those requirements be disregarded.

Even though Schwartz proceeds with caution over the propertization of personal data, he espouses a bundle of interests through inalienability, defaults, and a right to exit through the principle of consent, damages, and institutions.[40] As a result, his reluctance to support an IP right in personal data is offset by his contention that regulations are needed to redress the commodification of information, significantly but not exclusively through consent.

[35] *Ibid*, user-provided data are the only piece of information that is explicitly recognized as "commodifiable" as a kind of digital good of individuals. Indeed, it is the only set of personal data that can be "ported" from one platform to another. However, it is the only kind of (personal) data that the (proposed) law would consider a legitimate counter-performance other than money for the provision of digital content.

[36] Schwartz (2004), p. 7.

[37] *Ibid*.

[38] *Ibid*.

[39] *Ibid*.

[40] *Ibid*.

However, some commentators maintain that the problem with regulating the use of personal data lies in the fact that a person never fully owns or controls the use of their personal information once that person's data has a footprint on the Internet or network.[41] This is certainly true today, as the current regulatory framework whether in Australia, the EU or Singapore does not and cannot provide this level of coverage. The result is that data controllers and processors have the most control over personal data under current laws. Whether data collectors have rights that insulate their databases from regulation is increasingly in doubt, as regulators become increasingly aware of the abuse of such data. The unknown is how regulators can effectively regulate the collection and use of data in a technological era in which access to data is increasingly offset by technological means of avoiding such access. A further impediment is the lack of regulation afforded to the way in which hardware is regulated, arguably resulting in less protection of personal data. The resulting effect is that data protection law largely regulates the user. What is certain is that, despite these uncertainties, data controllers and processors are the primary beneficiaries of the value extracted from that data.[42]

Therefore, what is centrally at issue is the fact that data subjects do not truly own or control the use of their personal data throughout the cycle of use, commencing with a person accessing the Internet or network. The data subject's control over personal data is also likely to cease once that person has provided consent to the controller or processor of that data, whether or not the person consenting is informed about the consequences arising from its use, including by downstream users with whom the data subject has no contractual relationship.

The problem is that competing economic views of whether to add IP protection to the privacy of personal data are not conducive to reaching a universal outcome. Such divergent views reflect different responses to the expansiveness of personal data in a constantly evolving technological revolution, while policy makers emphasize different socio-economic and legal consequences arising from the commercialization of that data. Those who seek to protect personal rights from economic exploitation, like Professor Dorothy Glancy,[43] argue that personal information is at risk as it moves from the person who creates the personal information into files and databases of personal information controlled by others.[44] However, Glancy contends that, before imagining a speculative IP regime for personal information, it is essential to keep in mind that the socio-economic value of personal information warranting legal protection varies considerably across legal jurisdictions. Even though the protection accorded to personal information is defined in law, that legal definition diverges according to competing perceptions of the socio-economic value of protecting personal data.[45] Moreover, that legal definition fails to cover all software systems that capture one's personal data, often exposing that data to ongoing abuse. There is

[41] *Ibid.*

[42] Karanasiou and Douilhet (2016).

[43] Glancy (2010). The article recounts a thought experiment into what recognition of personal information as IP might look like.

[44] *Ibid.*

[45] *Ibid.*

a positive result, namely, growing recognition that the legal protection of that person's data is necessary to offset its abuse for profit.

Given divergent legal definitions and attributes accorded to data protection, an experimental model of data protection can help to determine how to extend IP protection to personal data. Some advances in this experimental direction are already reflected in existing literature, such as in evaluating when it is appropriate to treat personal information and the right to privacy as IP. Reaching that determination includes being able to identify the circumstances in which that personal information is most likely to be mishandled. On the one side in answering this question is that personal information is economically valuable, particularly to data collectors, data miners, and personal data merchants. On the other side is the need to evaluate the unjust enrichment implications of its use, such as when it is unfair for personal data collectors to capitalize on an asset that would not exist but for the person whose personal information is being handled, or mishandled.

Lawrence Lessig's instrumentalist theory of propertization does provide an economic argument for recognizing property rights in personal data, beyond IP rights.[46] Lessig argues that property rules would allow individuals to decide what information to disclose and what information to protect for privacy reasons. His rationale is that information privacy would provide greater control over personal information.[47] Supporting his view is the gradual shift towards tighter legal controls exerted on the collector and user of personal information. Lessig maintains further, that having property rights in personal data, will increasingly force businesses to negotiate with the individuals whose personal data is in issue. This propertization of personal data, he argues, will alter the architecture underlying the use of personal data, and will encourage greater investment in developing legally supported software systems to protect that data.

Litman agrees by maintaining that the position advanced by Lessig corresponds to the current legal position.[48] In effect, propertizing personal information[49] requires the inalienability of property in a legal system that protects privacy.[50] This leads to the hybrid inalienability of personal information, consisting of a use-transfer restriction, plus an opt-in default.[51] The hybrid inalienability of personal data, in turn, permits an initial transfer of that data from the data subject to the data collector, but only if the data subject is granted an opportunity to block further transfers or uses by unaffiliated entities. This is achieved through the concept of consent that enables the data subject to control how her/his personal data is used.

Importantly, in economic terms, scholars like Calabrese define property as opposite to the liability rule.[52] If any entitlement, whether to protect personal data or

[46] Lessig (1999).

[47] *Ibid.*

[48] Litman (2000), p. 1295.

[49] *Ibid*, p. 1283.

[50] Schwartz, *supra* note 36 p. 2097. Susan Rose-Ackerman's definition, an "inalienability" is "any restriction on the transferability, ownership, or use of an entitlement. Rose-Ackerman (1985), p. 268.

[51] *Ibid.*

[52] Calabrese and Melamed (1972).

not, is protected by a property rule, it cannot be taken away.[53] While the property rule protects any entitlement, the liability rule allows the data subject to transfer the liability or responsibility to a third party.

Today, to some degree, data protection law has followed the model espoused in Lessig's *Code*, as "the set of protocols … or rules, implemented, or codified, in the software of cyberspace itself, that determine how people interact, or exist, in this space."[54] Lessig elaborates by describing the law engaged in different methods of regulating markets in personal data.[55] These methods include direct regulation through the threat of punishment, and indirect methods of regulation through other legal constraints imposed by governments.[56] As a result, legal regulation includes different norms of regulation, different methods of regulating the market, and different architecture used to so regulate.[57] On the one side, direct regulation defines personal data, along with the concept of consent. On the other side, direct forms of regulation have spurned indirect forms of regulation in which data subjects have different levels of control and ownership over their personal data.

Nonetheless, the emergence of property rules, as distinct from liability rules, is not a new legal development. Scholars since the 1970s have grappled with introducing property rights in personal information, including to protect against economic abuse of that information.[58] Some have argued that, under natural law theory, there is an inherent connection between property rights in personal data and protecting personal data through those rights.[59] The modernized rationale is that this connection would help individuals to gain control over their personal data.

What is less readily appreciated is that regulating the use of personal data through IP rights in that data is different from regulating through general principles of property law. A property right, as distinct from an IP right, provides legal protection to whosever owns that property. If that owner is the data subject without whom there would be no data, a property right, arguably, would protect that subject's right in that data. However, that result is not necessarily so. It is also arguable that the first owner ought not to be data subject, but the first data collector because without that collection, the data would not exist on the Internet of Things.[60]

Whoever is deemed to be the owner of personal data, a property right in data is unduly absolute in nature. Given the digital expansion of interconnected and interoperable data, treating digital data as the legal object of a property right provides the data owner with an absolute ownership right, without identifying

[53] *Ibid.*

[54] Lessig (1998). Lessig argues that the *code* simply means the software and hardware that constitutes cyberspace as it is – the set of protocols, the set of rules, implemented, or codified, in the software of cyberspace itself, that determine how people interact, or exist, in this space … For the rest of us, life in cyberspace is subject to the code, just as life in real space is subject to the architectures of real space.

[55] *Ibid.*

[56] *Ibid.*

[57] *Ibid.*

[58] Agre and Rotenberg (1997).

[59] Solve (2001), pp. 1440–1446.

[60] Ciani (2018), pp. 285–291.

conditions under which that right can or cannot be exercised.[61] The further problem arises from bundling an array of different kinds of property rights under the broad umbrella of property.[62] The result is to complicate the very meaning of property and diminish its value in regulating the use, not limited to the purchase and sale, of personal data.

A further complication is that general property rights diverge across legal systems, as well as in jurisdictions that adhere to the same legal system. In contrast, IP rights are usually less diffuse across jurisdictions and are often developed with their extra-territorial application in mind.

Relying on contract rights to protect the personal information of data subjects is also deficient. For example, restricting the subject's protection in selling that data through a transfer or licence agreement raises the question as to who has a contract right in that data, the data subject or the first collector of that data. Linked to this is a more fundamental question: Who may sell personal data?[63] A strictly contractual approach limits the rights of data subjects over their personal data to their contractual relationships with data users, relationships which are often absent when data collectors bundle such personal information. A particular result is that data subjects who do not have contractual rights to that data are unable to regulate third-party use of their personal information.[64] Given the prospective number of data users, it is also difficult to identify the contracting parties to a data sale, the terms of the applicable contract, whether the seller is entitled to sell the data, and whether there are non-contractual protections available to either party.[65] Accentuating the limitation of contractual consent to collect, process or otherwise use personal information, is the fact that contractual self-regulation of data transactions is ordinarily dominated by data collectors and processors, and not data subjects. The reality is that dominant collectors and processors are likely to extract contractual concessions from data subjects who do not understand complex contract terms, such as those that exclude or limit the liability of dominant data collectors and processors. Nor, too, will most data subjects appreciate how such contracts will entitle data collectors and processors to use their personal data, including selling that data to third parties. The underlying problem is that data collectors and processors often have significant economic incentives to mislead data subjects by inducing them into one-sided contracts. Not only are the terms of such contracts seemingly ironclad, but most data subjects simply cannot afford to challenge them.[66]

As a result, treating personal data as general property, or information that can be exchanged by contract are imperfect means of regulating the abuse of that data. Whether one adopts a propertied or contractual approach to data protection, the architecture of cyberspace makes the collection of personal information difficult to

[61] Van Erp (2017), pp. 235–236.

[62] Sonnekus (2014), pp. 130, 136.

[63] *Ibid*.

[64] For arguments to the contrary, *see* Ciani, *supra* note 60, p. 288.

[65] *See* van Erp, *supra* note 61, p. 288.

[66] See the EU, General Data Protection Regulation 2016/679.

identify, and extremely difficult to control the use of that information. Indeed, data users can avoid detection by altering the source and use of such personal information. They can also employ propertied and contractual rights to impede efforts to control the abuse of such information.

Moreover, IP can accommodate both propertied and contractual rights. The importance of this argument lies in the fact that IP rights recognize property rights, such as to protecting copyright in data. IP rights also protect contract rights, such as through copyright and licensing agreements. However, it is important to differentiate between general property rights and IP rights, such as copyright, that is misdescribed as "property". IP is more aptly described as a distinct entity which includes conceptions of ownership, while also constituting a *sui generis* category of contracts.[67] As such, copyright laws regulate personal information less self-evidently through general principles of property law than through the exchange of contract entitlements. While IP can protect property rights, such as copyright, such property protection is ordinarily regulated by contract.[68] This predominance of contract over property is even more evident in relation to licensing agreement(s).

None of these benefits associated with IP are infallible. IP is often identified with the protection of creative ideas, while most personal data falls short of a creative idea. However, it is arguable that the protection of creative ideas is premised upon the need to avert threats of commercial exploitation. Similarly, trade in personal data is premised on a comparable need to avert threats to users who exploit personal information for profit.[69]

Ultimately, the *raison d'être* of an IP right in personal information is not only about its alienability, but also how it is bought, sold, and otherwise exchanged. Conceiving of the right to personal data as property *stricto sensu*, the purpose of property law is to prescribe the conditions for its transfer.[70] The concern is that property gives the owner of that property control over that data, including the right to sell or license it. That control includes the right to exclude the very person whose private information is being sold to third parties. The abuse of the exercise of that control through property is therefore necessarily subject to regulation. That regulation is provided through private remedies, such as quasi-property rights to privacy,[71] and by government regulations protecting privacy by operation of the law. The question is whether these private and public regulations provide adequate protection for data subjects whose information is bought and sold in the data markets of cyberspace, and whether an IP might fill lacunae in this infrastructure.

---

[67] *See e.g.* Lemley (2004), pp. 1–2.

[68] Van Erp *supra* note 61, p. 240 "A person's estate is comprised of all physical things and all patrimonial rights. However, a patrimonial right (e.g., 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.".

[69] *Ibid.*

[70] Litman (2000), *supra* note 48, pp. 1295–1296.

[71] Scholz (2016), pp. 113.

Adopting a constrained conception of IP rights can assist in reconciling principles of contract and general property. IP can also link the definitions of both personal data and privacy within national and supranational laws. IP protection also affirms the value of contract rights. Individuals can have a certain level of control over their personal data arising from their consent to its use. In fact, based on Litman's conception, the individual's consent to the use of her/his personal data is based on that individual's right to trade in that property.[72] Scholz, in turn, identifies a person's privacy rights with quasi-property, somewhat in line with Litman's view.[73]

Schwartz argues that the inalienable of rights in personal data is of the greatest value in restricting the transfer of rights in personal data, namely by combining restrictions in the use of personal data that also limit the transferability of that data.[74] That is, data subjects are provided with a level of control and ownership over their personal data through a combination of property and contract. That combination enables data subjects to restrict the use of that data. Economists and privacy advocates, in turn, have proposed giving individuals property rights in their personal data.[75]

However, granting individuals general property rights in their personal information, is unlikely to achieve all information privacy goals. This is because a key mechanism of property law, namely the general policy favoring free alienability of such rights, would more likely defeat than achieve information privacy goals. For example, Pamela Samuelson argues that providing greater protection to personal data in cyberspace and elsewhere is necessary to redress the incentives of the company that acquires private data, including personal data, to use it for profit.[76] Furthermore, the incentive to use that data includes the benefit of that company being able to use that information in its marketing efforts and to profit from its sale to third parties. Were the data subject to have a wholly inalienable property right rather than a quasi- property right, that company would not benefit from being able to disclose the inalienable private information of its customers freely to third parties. That restriction on transferability would also help to redress that company's incentive to internalize its gains from using such personal information, while externalizing losses, providing it with a systematic incentive to overuse that information. Conversely, if the right in data subjects is grounded in privacy and not property rights, and the company discloses that personal information at will, the result will be the potential over-disclosure of that information which data subjects would have difficulty remediating in law.[77] However, Samuelson bases her argument somewhat in the inalienability imputed to a right to privacy, and explicitly warns against propertizing personal information as a way of protecting the personal information of data subjects. It is Samuelson's rejection of arguments for protecting the property rights of data subjects with which this paper diverges.

[72] *Ibid.*

[73] *Ibid.*

[74] *Ibid.*

[75] Samuelson (2000), p. 1125.

[76] *Ibid.*

[77] *Ibid.*

It is justified to argue that a general property right is potentially too stringent in protecting personal data, particularly when a data user can freely use that data without control if it has such a property right. It is also not justified to argue for a general property right inhering in the data subject because this could result in undue constraint over the free flow of information and undermine the public's right to know. But these justifications are less compelling if the data owner enjoys an IP right which encompasses a level of control of that data falling short of an inalienable property right by including a conception of contract. In particular an IP right, as distinct from a general right can accommodate the right of data subjects to sell their personal data, such as through a licensing agreement, while not necessarily foregoing all copyright included by retaining IP rights against downstream users.[78]

Notwithstanding the authors' views, tensions remain between data protection and IP rights and property rights generally.[79] Of note, in many countries, personal data may be easily collected, both by using new technologies without the person being aware, and thereafter by selling, licensing, or using that data to create new IP-protected products. Data users can accomplish the latter result by incorporating that data in databases and, thereafter, by licensing it as part of a broader IP package.[80] This raises the issue of alternative means by which states can protect personal data, including means not yet explored above. One such means of protection is through human rights.

2.1.2 The Protection of Personal Data as a Human Right

For human rights advocates, it may seem wrong to consider personal information or privacy as general property because to do so is to treat the person who is the subject of that right as just an asset, or asset-generator. Moreover, to the extent that rights to freedom of expression include rights to collect and to communicate information, they include the right to collect and communicate personal information. Therefore, recognizing personal information as IP may undermine, not only the freedom to trade in that information, but also the public's right to have access to that information. Protection of personal information as IP would, as Glancy argues, be used to withhold important information from public discourse, especially personal information that relates to politically and economically powerful people about whom the public has a "right to know".[81]

Further justifications for not protecting personal information as IP is the argument that there are alternative ways in which to protect personal information, such as through regulatory measures, contractual agreements, the right to damages and other means. In other words, creating yet another form of property, here IP, would be ill-advised in further proliferating the legal protection personal information, despite limitations in these pre-existing measures.[82]

---

[78] *Ibid.*

[79] Karki (2005), pp. 59–62.

[80] *Ibid.*

[81] Glancy, *supra* note 43.

[82] *Ibid.*

However, some scholars resort to IP rights to protect personal data, combined with protection provided by other rights. Glancy argues that personal information is initially the intangible IP of the person who creates it. This personal information is frequently mixed thereafter with the IP rights of others in what amounts to a co-ownership arrangement. Her suggestion supports the development of appropriate IP rules to address the protection of personal information as IP, while recognizing its economic value to others.[83] The issue for Glancy is whether existing protections could be generalized into a more comprehensive IP right in personal information. Her response is in the negative on grounds that there are alternative ways to protect personal information that are more effective, such as through regulatory measures, contractual agreements, damages and other means, as well as her objection to proliferating IP rights.[84] In other words, further proliferation of forms of IP are ill advised.[85] We agree with Glancy's approach. Establishing rules of IP that are directed specifically at protecting personal data would serve to balance the rights of data subjects, while not stifling public access to that information. We also agree that relying on multiple forms of IP to protect personal data would create confusion, especially for data subjects, and potentially undermine data protections, or alternatively, the free flow of data.

The result of these different scholarly views is disquiet over why, when and where IP rights in personal data ought to exist, if at all. This raises further issues for policy and lawmakers over the applicable policy, principle and rule to adopt, such as in establishing when an IP right commences and concludes through the data use lifecycle. A further challenge for policy makers is to decide how far to extend the cycle of regulation in protecting the data subject's IP. Regulators who purport to regulate users along the full data use cycle are likely to protract the regulatory regime, rendering it unduly costly and ineffective to apply in a complex data environment. Conversely, restricting that regulation to the relationship between the data subject and the immediate data collector is likely to encourage the abuse of the data subject's personal information further down the data user cycle.

Yet another hurdle to overcome is whether to regulate personal data by contract, tort, or as IP, though a combination of these regulatory measures, or by invoking them separately. Regulating personal data contractually is likely to restrict the data subject's legal recourse to the immediate data collector or processor only, unless consent is construed expansively to encompass third-party users, or by subjecting the latter to tort claims, or conceivably, criminal liability. Treating personal data as IP is likely to extend regulation over the full lifespan of data usage. Especially if the specific IP right that is applied has an extensive lifespan.

Ultimately, there is no easy answer to these competing means of protecting personal data, other than by weighing the normative value accorded to the regulatory measures invoked to protect data subjects against the cost of such measures. This cost–benefit analysis arises whether policy makers conceive of IP as nothing more than another series of property, or as quasi-property that encompasses contract, privacy and other rights.

[83] *Ibid.*

[84] *Ibid.*

[85] *Ibid.*

2.1.3 Privacy Enhancing Technologies

Privacy enhancing technologies have advanced significantly over the past two decades.[86] They have been summarized as oriented around the subject, object, transaction and system.[87] This paper does not explore all the privacy enhancing technologies available, such as encryption, remailers, and Java Anon Proxy.[88] It stresses, rather, how these privacy enhancing technologies can enable data users to better protect their identifiable personal information. It recognizes that these protections are not infallible.[89] It also appreciates that these enhanced technologies are not necessarily subject to effective legal protection, whether through property, contract or IP rights.

What is increasingly feasible is the development of technologies that are accessible to consumers. Systems, such as the Midata Project announced in the United Kingdom, represent multi-stakeholder approaches to boost consumer empowerment by giving them increasing access to their personal data in a portable, electronic format. This enables data subjects to use such a system to gain insight into their own behavior, to make more informed choices about products and services, and to manage their economic lives more efficiently.[90] Mydex and HatDex have also developed a community platform model to build PDS (Personal Data Stores) that enable users to manage, share and deploy their personal data.[91]

Despite these developments, further technological developments are required to strengthen privacy and data protection more pervasively. There is a need to address issues surrounding the principle of transparency in the use of personal information and data, including through the ownership of such information.[92] Janeček maintains that, until the necessary technological advancements are available, ownership-like protection of personal data will remain fragmented. He argues that until such advancements eventuate, full ownership of personal data will remain both

[86] Goldberg (2018).

[87] Huberman et al. (2018).

[88] *Ibid*.

[89] The EU has taken the use of privacy enhancing technologies to protect the personal identities of users a step further than the other jurisdictions identified below. Article 25 of the GDPR adopted by the EU includes the principle of data protection by design. This requires that data controllers and processors adopt and embed privacy measures, including privacy enhancing technologies, directly into the design of technologies and systems. Cambridge Analytica harvested data from more than 87 million Facebook users, a whistleblower says, http://www.abc.net.au/news/2018-04-18/cambridge-analytica-employee-testifies-before-uk-committee/9670192, (accessed 2 August 2018). Notwithstanding Art. 25 of the GDPR, regulation of the Internet market has already failed to provide adequate technological mechanisms for coordinating individual wishes for information privacy. This inadequacy stems, in part, from evidence of a high number of privacy breaches on the Internet that are detected only after the fact, and then reported to national governments. For instance, the 2016 Facebook and Cambridge Analytica privacy breaches have all received worldwide attention from government regulators.

[90] Department for Business and Innovation Skills (2011).

[91] Mydex (2018).

[92] Janeček (2018).

technologically and legally unresolved.[93] Such fragmentation in detecting data abuse is also likely to pose ongoing challenges to policy makers and regulators. In particular, even if data subjects are treated as legal owners of their personal data, they are unlikely to ever identify whether their property or IP has been stolen, misused or damaged. Nonetheless, given current laws, emerging case law and technologies, there is an increasing argument that personal data, and as a consequence privacy, does fall under the rubric of IP to different degrees in the jurisdictions under study. The next sub-section will highlight how the laws of Australia, the EU and Singapore have defined personal data, as a prelude to evaluating its legal protection as IP.

2.1.4 Competing Definitions of Personal Data and Information

One of the first steps to understanding the relationship between personal data and IP in the EU, Australia and Singapore is to consider how each jurisdiction defines personal data and personal information. In particular a key issue is to determine whether the definition of personal data in these three jurisdictions enables data to be treated as IP, or as property in general. Significant differences in the definition of personal data/information in the EU, Australia and Singapore are outlined below.

All three jurisdictions include as personal information, the name, date of birth, and residential address of the data subject. Australia and Singapore specifically state what is personal data and how it is defined. Australia includes in its general definition of personal information and data, a person's full name, alias(es) or previous name(s), date of birth, sex, current or last-known address, and driver's license. Unlike Australia, neither the EU nor Singapore specify a person's alias or previous name in their general definitions of personal information. Defining personal information and data as including such information as a person's name and date of birth is not new and is not created by technology because that information is attributed to a person at birth and on being named. However, as technology has emerged, the ability to capture this and further personal data *en masse*, has significantly increased. Without that information, identifying the data subject accurately and comprehensively would be significantly greater.[94]

The EU takes a slightly different approach to both Australia and Singapore in defining personal data. The use of the term "personal data" in the EU is particularly significant, given the advent of new technologies in the 1970s that resulted in easily accessible datasets that were the catalyst for the EU establishing a comprehensive data protection framework.[95] Article 4 of the General Data Protection Regulation (GDPR) states that personal data means any information relating to an identified or

[93] *Ibid.*

[94] Interestingly, an important source of information identifying a person includes the current and last employer. As an illustration, once a person in Australia begins working or undertaking business, regardless of age, he/she is required to have a Tax File Number, even though a Tax File does not capture that person's identity to the same extent as an identification card that is required in Singapore.

[95] Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data*, European Commission (20 June 2007), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.

identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[96] This all-encompassing definition in the EU's GDPR captures personal data that is both general and that which other jurisdictions consider to be "sensitive". A material issue is whether there is a stronger case for an IP right to be afforded to sensitive personal data than general personal data.

2.1.5 Sensitive Information

Conceiving of personal data as sensitive arguably places this data in a category of its own. It is our view that this personal data requires a higher level of protection than non-sensitive (general) data, including through a purposefully framed IP right.[97]

Of the three jurisdictions, Australia is the only jurisdiction that defines "sensitive" personal data. It identifies that data with racial or ethnic origin; political opinions; membership of a political association; religious beliefs or affiliations; philosophical beliefs; membership of a professional or trade association; membership of a trade union; sexual orientation or practices; criminal record; health information about an individual; and genetic information (that is not otherwise health information).[98] In addition, Australia includes as sensitive information, biometric information that can be used for the purpose of automated biometric verification, or biometric identification.[99]

Singapore has grouped sensitive personal data with general personal data.[100] Apart from the full name of the person, Singapore has established mechanisms and systems that can identify people easily, such as the National Registration Identity Card (NRIC). Singapore is also the only jurisdiction to identify a passport and mobile phone number as part of a person's identifiable information. Additionally, Singapore has limited such data to facial images, voice recordings, fingerprints, iris images and DNA profiling.

The EU, rather than defining "sensitive data", has adopted a broad approach in identifying personal data, including what other jurisdictions have defined as being sensitive in nature. The EU concentrates significantly on the processing of personal data.[101] However, not wholly unlike Australia, it identifies personal data with information that reveals a person's racial or ethnic origins, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of

[96] *Ibid.*

[97] *See* Wang (2017), pp. 3286–3305.

[98] Privacy Act 1988, Sec. 6.

[99] *Ibid.*

[100] Personal Data Protection Act 2012.

[101] General Data Protection Regulation, Official Journal of the European Union 2016/679.

genetic or biometric data.[102] In effect, Singapore's identification of personal data includes, but is not limited to, data which Australian law treats as "sensitive".

Despite the divergent definitions of "sensitive data" in these three jurisdictions, most of the personal data or information captured by their respective definitions are similar. In particular, they all respond to the fact that most personal information is tradeable, portable and able to be transported from one jurisdiction to another. Whether that information is defined as being "sensitive" or as part of a "general" definition of personal data, the definition alone will neither totally preclude nor treat all personal data as IP.

However, there is a subtle difference between protecting private information and protecting data that identifies a person. Janeček illustrates with difference by highlighting the distinction between information-centered privacy and data-centered (control) of personal identifying information.[103] According to Janeček, this issue is best summarized by the ECtHR in its analysis of the unique personal data in a human DNA sequence, in stating that:

> a human DNA sequence or human cellular samples "contain substantial amounts of unique personal data" and merely retaining them invades, without further justification, the fundamental human right to privacy under Article 8 of the European Convention on Human Rights from 1950.[104]

What the court highlighted is that this unique personal data contains private information and controlling it is therefore almost like controlling one's individual identity. Janeček argues that this type of personal data must be excluded from any definition of personal data for the purpose of ownership, even though this data represents the core type of personal data as defined by the GDPR.[105]

On the other hand, Janeček argues that tracking a data subject's personal through a GPS system, an IP addresses, or data held within that data subject's personal task manager, is subtly different to protecting personal-centered data from personal-centered information. There is a twofold dichotomy in the current data protection laws and the definitions of personal data, along with the legal concepts and principles underlying them. First, data protection laws define what constitutes personal data or personal information. Secondly, the definition of personal data alone has created confusion in regulating it because no data is personal from the outset and all data can become personal.[106]

Janeček evaluates legal developments in personal data protection, starting with the relationship between the fundamental right to respect for private life, and the fundamental right to protection of personal data culminating in the data subject's rights granted by the GDPR in 2018. He maintains that this relationship, coupled with data as a source of identifying information, originates with information-centred

[102] Article 9, General Data Protection Regulation, Official Journal of the European Union, 2016/679.

[103] Janeček, *supra* note 92.

[104] *Id*, at 92, citing *Aycaguer v. France* App No. 8806/12 (ECtHR, 22 June 2017), (2017) EHRLR 519; *see also S v. United Kingdom* (2009) 48 EHRR 50 (ECtHR).

[105] *Supra* note 92.

[106] *Ibid*.

debate over the legal development of personal data protection.[107] The root of this problem is that the EU defines personal data in reverse: data is the source of information which, if that data is personal, implies that the original data is also personal. The clash between privacy and property assertions then looks like a chicken/egg problem in which it is unclear which of these two arguments comes first: information-centred privacy arguments that prioritize the personal chicken, or data-centred property arguments that highlight the egg.[108] However, there are conceptual and functional difficulties in distinguishing between personal information that is identified with privacy and personal data that is property-centred. The reality is that the data-centred property egg does not need to reveal or contain the personally centred information in every single case and can still can be considered valuable and worth protecting.[109] We may value data-centred property at different levels of abstraction than personal information. For example, an information-centred egg contains precious albumen as well as information about resistant constructions – you may try to crack it in your fist yourself.[110]

Data and information simply cannot be compared with each other at the same level of analysis because they are fundamentally different in characterization. On this account, Janeček contends that it is clear that personal and non-personal data are conceptually compatible.[111] He further highlights that there is a clash between information-centered privacy that cannot be owned and personal data that can, conceivably, be controlled. He asserts further that there is a need to restrict the potential scope of ownership and control over personal data "from an opposite direction", adding "[i]n that case the key question must be whether some data contains personal information intrinsically and therefore *cannot* be defined as non-personal data from the outset".[112] However, Janeček adopts a cautious approach that, since ownership of personal data still cannot be satisfactorily explained and justified as such, initiatives directed at data protection should remain investigatory, analytic, and descriptive, and not legally determinative.[113]

It is our view that Janeček's line of reasoning is somewhat circular primarily because control over personal data is provided for by law. Both data-centred and information-centred data have been defined, to varying degrees, by data protection

[107] *Ibid*. Janeček argued further that "[t]he original question featuring in said debates was 'When *information* (not data) can be protected by the law?' and the answer was that while semantic information (i.e. information per se) can never be protected by the law because it would violate free access to information, syntactic information can be given legal protection. From the information-centred viewpoint this answer was satisfactory. Saying that syntactic information or more precisely the formal expression of information, for example in form of a digital sequence of data, can be legally protected addressed the relevant information-centred problem. The data-centred discourse, however, cannot make efficient use of this conceptual scheme, because its original questions are 'How can we protect *data*?' and 'What information can be extracted from *data*?', not 'How can we express some *information* in form of (eg digital) data?'".

[108] *Ibid*.

[109] *Ibid*.

[110] *Ibid*.

[111] *Ibid*.

[112] *Ibid*, at 7.

[113] *Ibid*.

and privacy laws. Current data protection law strengthens the idea of information-centered privacy and data-centered property protection, although they do not fully remedy the issue of circularity identified above.

2.1.6 The Public–Private Divide

Another emerging challenge in protecting the rights of data subjects is the legitimate interest of an organization when it processes personal data, including balancing its commercial interests against other rights, not limited to the rights of a data subject. This balancing process will differ greatly between the public and private sector. Firstly, the public sector in most situations will be identified with the public interest, whatever that might be. However, in many countries the public sector contracts with private sector organizations to collect and process personal data on behalf of the public sector. This alone raises further issues over the actual or potential application of general property rights to personal data.[114]

The legitimate public purpose or interest approach is being considered by both Singapore[115] and Australia.[116] It is outside the scope of this paper to compare the different approaches these jurisdictions are adopting to evaluate whether and/or how to adopt this public interest approach. However, it is significant to observe they these countries consider the public interest in relation to the protection of personal data as sufficiently important to warrant further consideration.

3 Emerging Case Law

There is emerging case law in jurisdictions beyond the EU, Australia and Singapore, that demonstrate the propensity of courts to protect personal data through an IP right. Significantly, such protection extends beyond children to other vulnerable sectors of society, notably the aged. These developments are discussed below.

Courts in the United Kingdom have provided some direction on whether privacy can constitute IP. In 2012, the English and Wales Court of Appeal in *Coogan v. News Group Newspapers Ltd & Anor* ruled that confidential personal information is IP under Sec. 72 of the Senior Courts Act 1981.[117] In examining the construction of Sec. 72(2),[118] the court went to some lengths to explain IP in relation to the meaning of commercial information. It also maintained that the meaning of the expression "technical or commercial information" must be assessed by reference to the

[114] General Data Protection Regulation 2016/679, Art. 6 recognizes the legitimate interests by public authorities in the performance of their tasks.

[115] Personal Data Protection Commission (2018).

[116] Office of Australian Information Commissioner (2018).

[117] *Coogan v. News Group Newspapers Ltd* [2012] EWCA Civ 48, [2012] 2 WLR 84, [2012] EMLR 14, [2012] 2 All ER 74.

[118] *Ibid*.

purpose of Sec. 72, the immediate context in which that information is used, and the natural meaning of the words used.[119] Section 72 states:

> (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 IP or for passing off.[120]

The Court argued further, that IP covers confidential information. However, it maintained that it is unsatisfactory to place undue weight on a single generic term that covers all IP rights. In quoting from an earlier U.S. case, *Price v. Hal Roach Studios*,[121] the court reasoned that:

> [t]here is no single generic term that satisfactorily covers all rights which comprise intellectual property rights. However, the court went on to say intellectual property protects information and ideas that are of commercial value. The position taken by the court is that as long as the personal information is confidential and of commercial value it has a property right and can be treated as intellectual property.[122]

Price v. Hal Roach Studios[123]involved a dispute over the ownership of the commercial right to use the names and likenesses of Stanley Laurel and Oliver Hardy, the two famous but deceased comedians. The complaint was filed on 29 January 1971 by plaintiff Larry Harmon Pictures Corporation ("Harmon"), a California corporation, against defendants Hal Roach Studios, Inc. ("Roach"), a Delaware corporation with its principal place of business in New York, and Richard Feiner & Co. ("Feiner"), a New York partnership. Jurisdiction in the case was predicated upon diversity of citizenship. The plaintiffs, widows of Laurel and Hardy, and sole beneficiaries under their wills, claimed to have exclusive rights to their names and likenesses. The defendant asserted that, because the comedians were now dead, their names and likenesses were part of the public domain. They argued further, that the comedian's rights in their names terminated on their deaths, that these were property rights which were assignable in the public domain, and lived on in that domain.[124] The court decided that it might have been possible for the performers to have waived some of their rights to privacy while they were alive,

[119] *Ibid*.

[120] *Ibid*.

[121] *Price v. Hal Roach Studios*, Inc., 400 F. Supp. 836 (S.D.N.Y. 1975).

[122] *Ibid* [para 1-01].

[123] *Ibid*.

[124] *Ibid*.

in them being so well known by their names, but that the property rights in one's own name was not waivable.[125] In effect, the implication is that they had and retained a property right in their names which did not enter the public domain. The significance of this historical case lies in the fact that the current-day data protection and privacy laws in the countries studied in this paper, have defined a person's name as personal data that is subject to such legal protection. This protection conceivably includes a property right in one's name.

Consequently, the court in *Price v. Hal Roach Studios* did not focus on whether Laurel and Hardy's property rights in their names were analogous to *sui generis* IP rights. However, the court did demonstrate that, while they retained an inalienable property right in their names, they could waive some of their rights to privacy during their lifetimes. That waiver, implicitly if not explicitly, includes them granting third parties the contractual right to use their names.

4 A Pathway Ahead

IP in personal data, notably through the law of privacy, has emerged, particularly in the EU, but also in Australia and Singapore. While IP protection of personal data remains contested, recent developments in the EU and to a lesser extent, Australia and Singapore, indicate that such protection is becoming more important and more widely recognized by legislatures, courts and legal scholars. However, the protection of personal data is increasingly exposed to improved technologies that subject personal data to greater potential abuse in the data revolution of the 21st century. In response to *lacunae* in the protection of personal data, the EU has recognized the need to define and protect personal data, notably on grounds of privacy. Laws in the EU and elsewhere increasingly provide that such personal data is confidential. They acknowledge that personal data has a commercial value that warrants IP protection, commencing with the individual whose personal data is in issue.

Regulators and courts have also opened the door to such IP protection through the data subject's consent to use his/or personal data. They have enlivened the concept of implied or "deemed" consent, extending that consent beyond the first receiver of that personal data (the controller or processor) to downstream users. However, a requirement that the data subject consent to the use of personal data is distinct from that subject having an IP right in that data. An issue is whether such consent serves as a legal stepping stone from a contractual into a property right and specifically, into an IP right. Relying on consent to limit the use of personal data is deficient in the absence of a contractual right between the disputing parties. A data subject cannot withdraw his consent to downstream users of that data in the absence of a privity of contract between that data subject and those users. The result is that, if the consent of data subjects to the collection, processing and transmission of their personal data is deficient, the case for a property right, and arguably, an IP right in personal data, becomes more legally defensible. Alternatively, if consent is

[125] *Ibid*.

extended beyond express consent to implied or ostensible consent, data subjects (and first collectors of their personal data) could withdraw their consent to downstream users of that data.

However, what remains perceptibly lacking in regulatory schemes is the virtue of protecting the rights of the individual to personal data beyond the privity of contract between consenting parties. One means of doing so is by recognizing the IP rights of "owners" of personal data which is not readily forsaken by implying the consent of the data subject to transfer "ownership" of that data. Another is to regulate the transmission of such personal data along a chain of users whose use of that information was not reasonably foreseen by the data subject who consented to that use by the first controller or processor. However, courts may well hold that "deeming" consent, including its withdrawal, over-extends the scope of consent to contract, and ought not reasonably to be implied, or otherwise imputed by the data subject to downstream data users.

Another option is for governments to impose requirements on the use of personal information, beyond the consent of the individual, on grounds of a fathomable but not overly expansive public good. Regulators and courts have already, albeit limitedly, entertained such protection of personal data on public policy grounds. They have done so in protecting "sensitive" personal data, and in protecting the data of children, directly or by implication, under EU, Australian and Singaporean law. However, they have yet to redress conflicting conceptions of the public good that encourage the free flow of personal data to society at large, but that limit that flow to protect vulnerable individuals. This is particularly the case in a complex virtual world in which the average consumer is unlikely to be aware of how extensive his/her personal information can be used due to technological innovation that makes detecting data abuse ever more difficult.

However, resort to public law measures to protect personal data internationally presupposes a consensus among states that is politically and economically fraught. States have different reasons for supporting or denying protections to data subjects, based on their localized ideological, economic and political policies. They include, among others, an ideology that support a free market in the exchange of information, a state's reliance on revenue generated from data collectors and processors, and its public policy interest in, *inter alia*, national security, public health and social stability. They include the converse interest of governments not to constrain access to, or the use of, personal data in pursuit of revenues from data collectors and processors, notwithstanding the adverse human rights impact of that use upon data subjects.

What has also not been adequately explored is how to balance private and public interests in protecting personal data. There are four different factors to consider in engaging in such balancing. The first criterion is a free exchange in data. This presupposes that everything that appears on the Internet is public property. Everyone is free to use it, without needing to account for that use. Given that no one owns that data, and that no one has a contractual right to sell it, it can be used without restriction. One consequence is that the data subject's personal information is freely, and arguably unduly, accessible for public and private use.

Second and conversely, all data is owned. However, this scenario does not differentiate among owners of data. A data collector who owns data could deny the data subject any control over its use in a virtual world in which personal data has commercial value.

A third and tempered response is that data subjects are entitled to protection in the use of their personal data, such as through privacy or contract rights. However, this response requires an a priori determination that a data subject's privacy is under threat, or that the data subject has a contractual right to protect it from a breach of that contract by a data collector or processor. The data subject's contractual rights also do not ordinarily provide protection from downstream users with whom that subject does not have a contractual relationship.

A fourth response is regulatory, in relying on lawmakers and courts to regulate the use of personal data. The problem is that such regulation, no matter the jurisdiction, to date, has been selective, fragmented and far from universally adopted. A related consequence is that data subjects did not receive direct rights of action against data users who allegedly misused their personal data.

The result of these four methods of protecting, or not protecting, personal data is a smorgasbord of seemingly incompatible methods of using, protecting and regulating that data. Therefore, a purposive study is needed to determine the perceived extent to which personal data can be used and abused; the nature, source and extent of that abuse; the means currently employed to redress that abuse; the success of those means to date; and the prospects of adopting effective and fair measures to address deficiencies in those regulatory measures. This is increasingly becoming more important because of the convergence of data protection and cyber security. That is, the illegal collection and use of personal data is beginning to fall into the criminal domain. As this paper has demonstrated, the EU has gone furthest along this pathway in its 2018 GDPR. The pathway ahead is formidable. It is also potentially treacherous in recognizing the competing personal and commercial interests involved, and limitations in reconciling disparate regulatory measures.

The comparative analysis of legal developments in the EU, Australia and Singapore highlights a further challenge in the tension between common and civil law conceptions of ownership and control of personal data. Arguably, the common law provides greater flexibility in the types of ownership that can be created and protected as property rights.[126] The civil law, such as in EU jurisdictions, restricts the number of property rights and also subjects a limited number of legal objects to these property rights (*numerus clausus*).[127] As highlighted by Janeček, the civilian idea of ownership is an absolute dominion encompassing all the listed rights (*numerus clausus*) over the relevant object; whereas, in the common law tradition, ownership includes a variety of different rights over the same property.[128] The result is that, unlike in civil law, acquiring ownership in common law systems can be gradual. An individual or entity can have more, or less, ownership, depending on the

[126] Gordley (2006), p. 49.

[127] Akkermans (2008).

[128] Janeček, *supra* note 92.

size of that person's bundle of property rights in the data object.[129] A potential result is that the civil law is more likely than the common law to facilitate the development of property rights in personal data. The added impediment is that such divergence is likely to complicate attempts to arrive at harmonized solutions across these two globally predominant legal systems.

It is our view that, given the divergence between these legal systems, the pathway forward would entail greater legal convergence around key concepts and principles, such as in the definition of personal data and in consent to collecting, processing and other use of that data. This approach has, arguably, been successful in other areas of private international law, such as in international trade law. However, the challenge for policy makers in the field of data protection lies in the multi-layered approach and direction that data protection laws have assumed to date. Data protection laws provide data subjects with a threshold level of privacy rights, while further protections are emerging in other areas of law, such as contract, IP and competition law. The result is that data protection laws are doing many things for many people and many interests, but sometimes quite differently. The resulting regulatory framework is also reductionist as states seek to develop their domestic laws, including data protection laws, to meet localized needs and public policy. The end-product is the marginalization of transnational public policy, such as the modes of data protection that are ideally shared across state boundaries, rather than subordinated to divergent state laws. As highlighted earlier this is further complicated by the fact that sovereign states view privacy over the Internet differently, even though a shift has commenced and there is a general acceptance of privacy over the Internet. That said, it remains quite varied even amongst Australia, the EU and Singapore.

An important purpose in developing transnational data protection law is to address the extent to which personal information and data ought to be treated as property, and as IP rights in particular. The ability to balance the rights and control of data subjects against the rights of data users, is an unavoidable challenge for regulators and policy makers. How much control ought to be afforded to data subjects through the law is contentious. Whether that control extends to the first, second, third, fourth, fifth, or further point in the cycle of collection and use of personal data is an open question. The principles espoused by the OECD, particularly regulating transparency in data use and accountability for its misuse, provide a sound point of commencement. The issue is to determine how far they ought to be extended. These are also policy challenges that warrant ongoing scrutiny, such as how the regulation of personal data ought to reconcile private data rights with public interests in that data. Such policy issues impact upon the scope of both general property and IP rights for two related reasons. Public organizations use private organizations to collect and hold personal data, and data protection laws can be applied differently between public and private entities. How to devise and apply these laws transnationally and inter-jurisdictionally is far from clear at this juncture.

[129] *Ibid*.

5 Conclusion

Determining whether personal data is afforded IP rights, beyond general property rights, is contested. This contest is accentuated by the fragmented approach adopted by different jurisdictions in the development of data protection law. This paper has argued that personal data is beginning to be accorded property rights in personal data, and to IP rights as a distinct *genus* of property.

The paper argues that, with the ever-spiraling evolution of technology, according data subjects IP rights over personal data has distinct benefits. Firstly, in the contemporary world, personal data is increasingly a source of trade in cyberspace. Secondly, having an IP right in personal data reinforces, and expands the regulatory framework by extending greater control over the use and misuse of personal data. Thirdly, protecting personal data through IP rights is comparable to protecting commercial information through IP rights, a practice that has pervaded international markets for decades.

The paper has considered whether all personal data should be subject to comparable IP protection. Arguably, at a minimum, sensitive personal data should be afforded IP rights. The perceived problem in accomplishing this goal, as this paper has demonstrated, is that jurisdictions often fail to distinguish between sensitive and other personal data. Nonetheless, this divergence does not pose insurmountable obstacles, as greater uniformity could be accomplished through limited law reform. An alternative solution is to subject all personal data to IP rights, in recognition of the tradability in personal data. This option faces significant economic and political obstacles, given that restricting trade in personal data potentially undermines the profits earned by data collectors and processors who transact in such data. However, and conversely, politically it is likely palatable to accord IP rights to personal data, because it also enables greater certainty and stability in this emerging market.

The downside, in not affording data subjects IP rights to protect personal data from misuse is formidable, including diluting the emerging legal framework for data protection. Such legal developments, particularly in the EU, and to a lesser extent in Australia and Singapore, have provided data subjects with a level of control over their personal data, including by placing limits on how and when that data can be traded. Should data subjects be denied that level of control, the risk is that regulators will accelerate an already worrisome level of unfettered trade in personal data. The ancillary risk is that, in doing so, they will marginalize the rights and interests of data subjects whose personal data is the source of that trade.

Nonetheless, how far IP rights in personal data ought to be extended remains speculative. One measure of protection under development is to provide data subjects with greater control over their personal data, based on a principled level of ownership that is applied functionally to personal data. The problem is that, even though personal information may be the subject of IP rights, such as database rights and copyright protection, the information itself is not generally subject to protection as property. Moreover, so long as data is not distinguished from physical assets, that data is unlikely to be protected in an identical manner to the protection of physical property. However, if that information can be protected as IP, such as through

copyright and licensing agreements that allow it to be bought and sold (no matter where in the supply chain), there is a greater prospect of protecting personal data than under the general law of property.

The protection of IP rights in personal data is in an early stage of development, even though, personal information has been traded for decades. What is different is primarily the environment in which such trading occurs. Trading in personal data over the Internet takes place in a specialized environment involving its trade, potentially multiple times, through and to varying organizations. In effect, personal data identifies a single person, not unlike trading in personal information before the Internet era. Our technological new world order, dominated by the vicissitudes of cyberspace, is also increasingly recognized in current data protection law and judicial decisions. Regulators and courts have also demonstrated, albeit incrementally, a greater willingness to provide data subjects with some level of ownership and control, including through IP rights, over the collection and use of their personal data. They have recognized that IP rights can reconcile limitations in both the contract and general property rights of data subjects, providing those subjects with a staging platform on which to protect their personal information.

The EU's GDPR is already reinforcing the rights to data subjects to control access to their personal data. This has developed, in part, through the EU's introduction of the right to data portability and to data access. The EU has further emboldened the ownership of personal data in the legal definition accorded to personal data, and the application of the concept of consent to the use of that data. Data protection laws in Australia and Singapore have also provided data subjects with greater control over their personal data, albeit not to the same degree as in the EU.

An overriding concern is that the privacy of personal data is under growing threat of being traded and transferred on account of its inherently portable nature. The result, as highlighted by a recent case in the UK, is that personal data is now receiving greater judicial protection, including through IP rights. Supporting this development is the fact that both the definition of personal data and the concept of consent to data use have strengthened the argument that personal data ought to be protected as an IP right that includes both property and contractual components. Arguably, the right to access personal data, and in the case of the EU, the right to portability, have further reinforced the proposition that, imbedded in personal data, is a justifiable IP right to regulate that access.

Nevertheless, the challenges in endorsing IP rights to protect personal data, are formidable. The expanding requirement that data subjects' consent to the use of their personal data, including to withdraw that consent, provides them with greater control over that data. However, control over data is distinguishable from ownership, just as consent to the use of personal data diverges from having a property right in that data. Similarly, a conception of IP that includes privacy, consent and property rights can provide data subjects with effective and fairer protection of their personal data. However, it can also expose data subjects to data users who manipulate the variable attributes of those rights according to the machinations of the applicable law.

Notwithstanding these obstacles, there remain credible support for some level of IP protection of personal data. In responding to the extent to which individuals are

induced or deceived into consenting to wide access and use of their personal data, EU regulators have sought to protect that personal data from commercial or other uses that violate the privacy of data subjects, and arguably, undermine their IP rights. This regulatory response is most evident in the EU's GDPR, which is gradually being adopted elsewhere, such as in Australia and Singapore. Whether such developments have gone far enough is questionable. Whether they will evolve significantly further, to enhance both the privacy and IP rights of data subject, remains uncertain. However, there is credible reason to believe that data protection laws, including through IP, are being extended to sensitive personal data, not limited to the data of vulnerable sectors of society such as children. There is further evidence of a willingness by regulators and courts to construe the consent of data subjects to use of their data in the interests of those subjects. What remains contentious is the extent to which data subjects should be treated as "owners" of personal data in determining whether to retain, sell, or otherwise consent to the transfer of their personal data and whether there are circumstances in which third parties can use that data in the absence of their consent.

This paper has maintained that IP rights, rather than being a part of the problem, constitute an important part of the solution to the issues identified above. What is insufficiently understood is that IP rights are distinct from general property rights. More aptly referred to as "quasi-property" or "hybrid" rights, IP rights incorporate rather than exclude other rights, such as contract rights that inhere in copyright and licensing agreements. Conceived as "quasi-property," IP rights provide data subjects with the right to sell personal data, together with a residual property right to protect that data from downstream users with whom the data subject has no contractual relationship. The result is that data subjects can use such IP rights to protect their personal data more effectively than most legal systems that rely primarily on contracts to protect that data, even though data collectors and processors often use contracts to subvert that very protection. Regulators can also invoke IP rights to avoid the intransigence of general property rights in which strict conceptions of ownership potentially stifle the exchange of data in Cyberspace. What IP rights can provide, therefore, is a measure of regulation over the transmission and use of personal data, ensuring that data collectors, data miners, and data merchants are not wholly subjugated by inalienable property rights of data subjects. If policy makers are to achieve these balanced ends, they need to further develop both a principled and a functional IP framework in which to determine the boundaries of personal data protection. Encompassed within that framework is the importance of rendering data users accountable for how they collect, process, mine and transmit personal data, without stultifying the use of that data. While that framework should protect sensitive data, it should also accord data subjects with that level of protection over their personal data with which they are reasonably comfortable. Importantly, that regulatory frameworks should function transparently in a manner that is consistent with the principle of transparency as a cornerstone of data protection law, no differently to that of commercial data over the past 50 or more years.

References

Agre P, Rotenberg M (1997) Technology and privacy: the new landscape. MIT Press, Cambridge

Akkermans B (2008) The principle of numerus clausus in European property law. Intersentia, Antwerp

Berners-Lee T (2019) Interview on the need to seek complete control of data. https://www.channelnewsasia.com/news/world/web-inventor-urges-users-to-seek–complete-control–of-data-11334546. Accessed 12 March 2019

Calabrese G, Melamed AD (1972) Property rules, liability rules, and inalienability: one view of the cathedral. Harv Law Rev 85:1089–1128

Chesterman S (2012) After privacy: the rise of Facebook, the fall of Wikileaks, and Singapore's personal data protection act 2012. Singap J Leg Stud 391–415

Chesterman S (2018) Data protection law in Singapore, privacy and sovereignty in an interconnected world. Academic Publishing, Singapore

Ciani J (2018) Governing data trade in intelligent environments: taxonomy of possible regulatory regimes between property and access rights. Intell Environ 23:285–291

Cohen J (2000) Examined lives: informational privacy and the subject as object. Stanf Law Rev 52(1373):1423–1428

Department for Business and Innovation Skills (2011) The midata vision of consumer empowerment. https://www.gov.uk/government/news/the-midata-visionofconsumerempowerment. Accessed 28 April 2018

Dhanjani N (2015) Abusing the internet of things: blackouts, freakouts, and stakeouts. O'Reilly Media, Sebastopol

Glancy D (2010) Santa Clara personal information as intellectual property. https://www.law.berkeley.edu/files/bclt_IPSC2010_Glancy2.pdf. Accessed 20 May 2019

Goldberg I (2018) Privacy enhancing technologies for the internet III: ten years later. Cheriton School of Computer Science University of Waterloo. https://www.cypherpunks.ca/~iang/pubs/pet3.pdf. Accessed 26 April 2018

Gordley J (2006) Foundations of private law: property, tort, contract, unjust enrichment. OUP, Oxford, p 49

Huberman B, Franklin M, Hogg T (2018) Enhancing privacy and trust in electronic communities. Xerox Palo Alto Research Center, Palo Alto. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.89.395&rep=rep1&type=pdf. Accessed 26 April 2018

Janeček V (2018) Ownership of personal data in the Internet of Things. Comput Law Secur Rev 34:1039–1052

Karanasiou A, Douilhet E (2016) Never mind the data: the legal quest over control of information and the networked self. http://eprints.bournemouth.ac.uk/23392/1/PID4084429%20%285%29.pdf. Accessed 20 May 2019

Karki M (2005) Personal data privacy and intellectual property. J Intellect Prop Rights 10:59–62

Kozyris PJ (2007) Regulating internet abuses: invasion of privacy: invasion of privacy. Wolters Kluger, Alphen aan den Rijn

Lemley M (2000) Private property: a comment on professor Samuelson's contribution. Stanf Law Rev 52:1551–1554

Lemley M (2004) Property, intellectual property, and free riding. Stanford Law School, Working Paper No. 291 August 2004, pp 1–2

Lessig L (1998) The laws of cyberspace. https://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf. Accessed 2 Jan 2018

Lessig L (1999) Code and other laws of cyberspace. Basic Books, New York

Litman J (2000) Information privacy/information property. Stanf Law Rev 52:1295

Malgieri G (2018) User-provided personal content in the EU: digital currency between data protection and intellectual property. Int Rev Law Comput Technol 32(1):118–140

Merges P, Menell P, Lemley M, Jorde T (1997) Intellectual property in the new technological age. Aspen Law & Business, New York, pp 11–20

Mydex (2018) https://pds.mydex.org/. Accessed 28 April 2018

Office of Australian Information Commissioner (2018) https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts. Accessed 26 Oct 2018

Personal Data Protection Commission (2018) https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Legislation-and-Guidelines/PDPC-Response-to-Feedback-for-Public-Consultation-on-Approaches-to-Managing-Personal-Data-in-the-Dig.pdf. Accessed 26 Oct 2018
Rose-Ackerman S (1985) Inalienability. In: The new Palgrave dictionary of economics and the law. Yale Law School Faculty Scholarship, vol 1–3, p 268
Samuelson P (2000) Privacy as intellectual property? Stanf Law Rev 52:1125
Scholz L (2016) Privacy as quasi-property. Iowa Law Rev 101:113
Schwartz P (2004) Property, privacy, and personal data. Harv Law Rev 117:7
Solve D (2001) Privacy and power: computer databases and metaphors for information privacy. Stanf Law Rev 53:1440–1446
Sonnekus J (2014) The fundamental differences in the principles governing property law and succession from a South African law perspective. Eur Prop Law J 3(130):136
Tene O, Polonetsky J (2013) Big data for all: privacy and user control in the age of analytics. Nw J Tech Intell Prop 11:239
Van Erp S (2017) Ownership of data: the numerus clausus of legal objects. In: Brigham-Kanner property rights conference journal, vol 6, pp 235–236
Wang M (2017) The defining approaches and practical paradox of sensitive data: an investigation of data protection laws in 92 countries and regions and 200 data breaches in the world. Int J Commun 14:3286–3305
Warren S, Brandeis L (1890) The right to privacy. Harv Law Rev 4:193–220
Zittrain J (2000) What the publisher can teach the patient: intellectual property and privacy in an era of trusted privication. Stanf Law Rev 52:1203

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.