PRIVATE AND COMMON PROPERTY RIGHTS IN PERSONAL DATA

This article makes a case for examining personal data from a property law perspective. In particular, it sets out the arguments both in favour of and against granting private and common property law rights in personal data. While property law is not a panacea for all the problems that have arisen in the big data era, it provides a useful framework and a set of established principles for approaching those problems.

HU Ying[1]
LLB (The University of Hong Kong),
LLM (University of Cambridge & Yale Law School);
Lecturer, National University of Singapore.

I. Introduction

1 We find ourselves in a rather odd situation: companies collect and use data about our online and offline activities to make huge profits. However, there is no *prima facie* right for us to share any portion of that profit. Despite common belief that our personal data belongs to us,[2] we do not legally own that data, which is not even considered "property" in the first place. Unless otherwise specified, the term, *personal data*, is used broadly in this article to refer to information about an individual's characteristics, knowledge and behaviour – ranging from his gender and age, to his political affiliation and the time he goes to sleep at night.

2 Academics have long debated whether individuals should be given property rights over their personal data.[3] In recent years, the idea of

1 The author would like to thank Professors Lee Pey Woan, Daniel Seng, Tang Han Wu, Alvin See Wei Liang, Yip Man, Ernest Lim, Tan Zhong Xing, Tham Chee Ho, as well as other participants of the Third Asian Private Law Workshop, for their helpful comments. All mistakes remain the author's.

2 See, *eg*, an interview with European Competition Commissioner Margrethe Vestager, in which she said: "Because now we know that we all own our data." Jennifer Baker, "Vestager on the Intersection of Data and Competition" *IAPP* (30 October 2018) <https://iapp.org/news/a/vestager-on-the-intersection-of-data-and-competition/> (accessed 30 March 2020). Mark Zuckerberg also claims that individuals "own" and have "complete control" over the information they post on Facebook. Transcript courtesy of Bloomberg Government, "Transcript of Mark Zuckerberg's Senate Hearing" *The Washington Post* (11 April 2018).

3 See, *eg*, "Developments in the Law: The Law of Cyberspace" (1999) 112 Harv L Rev 1574 at 1644–1648; Jerry Kang, "Information Privacy in Cyberspace

(cont'd on the next page)

propertising personal data has gained greater public attention as various politicians proposed legislation seeking to grant individuals property rights over their data.[4] At the same time, a greater number of digital platforms have emerged to facilitate commodification of personal data.[5]

3 This article suggests that there may be advantages to treating personal data as property. Part II outlines both the benefits and harms that might result from the collection and use of personal data. Part III explains what it means to examine personal data from a property law perspective and the value of such an approach. Parts IV and V set out the arguments in favour of granting both private and common property law rights in personal data.

II. Personal data: A story with two sides

4 We live in the era of "big data". An increasing number of our interactions with the world are being tracked: the goods we purchase, the photos we post, and the places we visit are stored electronically by service providers such as Amazon, Google and Facebook. These tech giants are not alone in the quest for more data. Many websites track visitor Internet Protocol addresses, browsing histories, mouse movements and sometimes even battery states.[6] Entrepreneurs peddle "free" applications ("Apps") ranging from games to fitness trackers to record a greater variety of user data. This part highlights both the dark and the bright sides of ubiquitous collection and use of personal data.

Transactions" (1998) 50 Stan L Rev 1193 at 1246; Pamela Samuelson, "Privacy As Intellectual Property" (2000) 52 Stan L Rev 1125; Jessica Litman, "Information Privacy/Information Property" (2000) 52 Stan L Rev 1283; Paul M Schwartz, "Property, Privacy, and Personal Data" (2004) 117 Harv L Rev 2056; and Christopher Rees, "Tomorrow's Privacy: Personal Information as Property" (2013) 3 *International Data Privacy Law* 220.

4 For example, US Senator John Kennedy introduced a three-page Bill which declared that each individual "owns" and has "exclusive property right" in the data she generates on the Internet. The draft Bill is available at <https://www.govinfo.gov/content/pkg/BILLS-116s806is/pdf/BILLS-116s806is.pdf> (accessed 10 December 2020).

5 See, *eg*, Megan Molteni, "These DNA Startups Want to Put Your Whole Genome on the Blockchain" *Wired* (16 November 2018) <https://www.wired.com/story/these-dna-startups-want-to-put-all-of-you-on-the-blockchain/> (accessed 15 April 2020).

6 Antonio Villas-Boas, "Passwords Are Incredibly Insecure, So Websites and Apps Are Quietly Tracking Your Mouse Movements and Smartphone Swipes Without You Knowing to Make Sure It's Really You" *Business Insider* (19 July 2019); Alex Hern, "Your Battery Status Is Being Used to Track You Online" *The Guardian* (2 August 2016).

A. The dark side

(1) Loss of privacy

5 The rise of big data is likely to pose a significant threat to people's right to privacy. Scott McNealy, the chairman of Sun Microsystems, famously said, "you already have zero privacy – get over it".[7] While privacy is a notoriously difficult concept to define, this article focuses on what has come to be known as information privacy, which is often understood as a person's "control of information concerning his or her person".[8]

6 Big data undermines our control over our personal data in a number of ways. First, we are more likely to experience difficulty determining when our data is being collected. Technologies such as cookies and web beacons allow websites to track their visitors unobtrusively. When we walk on a street, we often know when we are being followed. However, it is much more difficult to detect a follower online: for example, many people did not know that the mere presence of a Facebook "like" button meant their online activities were being reported back to Facebook.[9]

7 We are also more likely to be mistaken about who has access to our data. What appears to be a one-on-one interaction can sometimes involve hidden third parties. When buying a prescription drug from an online pharmacy, we tend to assume that we are dealing only with that pharmacy. However, the pharmacy might allow third parties to store cookies on its website, alerting them to our visit. It might even sell information about our purchase records: Pharmacy2U, the UK's largest NHS-approved online pharmacy, was fined for selling customer data (at the price of £130 per 1,000 customers) without their consent.[10]

8 Moreover, we often do not know when we disclose more information than we intend to. If we upload a photo taken with our smartphone, we might not know it is embedded with a geotag that can reveal our location.[11] Businesses also increasingly use algorithms to

---

7 Amitai Etzioni, "Privacy Isn't Dead Yet" *The New York Times* (6 April 1999).

8 See, *eg*, *US Department of Justice v Reporters Committee for Freedom of the Press* 489 US 749 at 763 (1989).

9 Riva Richmond, "As 'Like' Buttons Spread, So Do Facebook's Tentacles" *BITS* (27 September 2011) <https://bits.blogs.nytimes.com/2011/09/27/as-like-buttons-spread-so-do-facebooks-tentacles/> (accessed 10 December 2020).

10 Dave Lee, "Online Pharmacy Fined for Selling Customer Data" *BBC News* (21 October 2015).

11 Kate Murphy, "Web Photos That Reveal Secrets, Like Where You Live" *The New York Times* (11 August 2010).

analyse our data to find correlations and patterns of behaviour. A famous example is Target's prediction of a girl's pregnancy, from her shopping history, before her family was aware of it.[12] Sometimes, additional personal information may be deduced from seemingly unrelated data. In one study, researchers demonstrated that Facebook "likes" could be used to predict a wide range of personal attributes.[13] Interestingly, among the content "liked" by Facebook users, the best predictors of high intelligence include words such as "thunderstorms" and "curly fries".[14] Consequently, it is difficult for us to know what insights businesses can generate from the information we have disclosed, the accuracy of those insights, or how they might be used against our interest.

(2) Data-related harm

9 The personal data we have disclosed, either intentionally or unintentionally, can be used to our disadvantage in various ways. For example, information about an individual's location might enable criminals to stalk or injure him. A few years ago, an App called "girls around me" used information from Facebook and Foursquare to display images of nearby users.[15] One can easily imagine the physical danger this App posed to the girls whose images and locations were captured by the App. Not surprisingly, there was a backlash against it.[16] Our personal data might also enable retailers to charge us a higher price than they would charge someone living in a different neighbourhood: for example, in the US, the prices for The Princeton Review's online SAT tutoring packages varied significantly depending on the location of its customers; moreover, customers in Asian-majority neighbourhoods were almost twice as likely to be offered higher prices.[17]

10 Further, the personal data that companies have collected about an individual as well as inferences made based on such data might be inaccurate or outright false, causing that individual to suffer reputational damage, emotional distress or financial loss. Even where the relevant information or inferences about an individual is accurate, it may

12 Charles Duhigg, "How Companies Learn Your Secrets" *The New York Times* (16 February 2012).

13 Michal Kosinski, David Stillwell & Thore Graepel, "Private Traits and Attributes Are Predictable from Digital Records of Human Behavior" (2013) 110(15) *Proceedings of the National Academy of Sciences* 5802.

14 Michal Kosinski, David Stillwell & Thore Graepel, "Private Traits and Attributes Are Predictable from Digital Records of Human Behavior" (2013) 110(15) *Proceedings of the National Academy of Sciences* 5802 at 5804.

15 "Privacy Backlash Over Girls Around Me Mobile App" *BBC News* (2 April 2012).

16 "Privacy Backlash Over Girls Around Me Mobile App" *BBC News* (2 April 2012).

17 Julia Angwin, Jeff Larson & Surya Mattu, "Test Prep Is More Expensive – For Asian Students" *The Atlantic* (3 September 2015).

nevertheless be used to discriminate against that individual, to exploit his vulnerabilities, or to manipulate his behaviour (*eg*, his voting decision).[18]

B. The bright side

(1) Personal data fuels the economy

11 On the other hand, personal data has been the backbone of many technology companies. Facebook alone made a profit of US$1.6m in the last quarter of 2015, the majority of which was derived from advertising programmes.[19] The wealth of data controlled by Facebook enables advertisers to target specific groups of people based on their location, demographics, interests and behaviour (*eg*, female lawyers aged 20 to 30, living in San Francisco, who eat organic food and have purchased gym memberships in the past year).[20]

12 Companies also increasingly devote resources to analysing personal data in order to generate more profits. Such analyses sometimes enable them to better anticipate the needs of their customers: in the case of Target, after concluding that a girl was pregnant from her shopping history, it sent her coupons for baby clothes and cribs.[21] Other times, insights from personal data help companies reduce operation costs: thanks to the petabytes of customer data in its warehouse, eBay manages to automate 90% of the 60 million disputes it receives every year, thereby saving hundreds of thousands of dollars in labour costs.[22]

(2) Personal data is essential to technological development

13 Personal data has played and will continue to play an essential role in developing new products and services through machine learning. Machine learning models are often trained with large datasets, a significant part of which is personal data. Our medical data, for example, may be used to help diagnose genetic diseases earlier and with

18 See, *eg*, Jack M Balkin, "The Three Laws of Robotics in the Age of Big Data Lecture" (2017) 78 *Ohio State Law Journal* 1217 at 1237–1238 (identifying five types of harm caused by algorithmic decision-making).

19 Hope King, "Facebook Is Making More Money Off You Than Ever Before" *CNN Business* (27 January 2016).

20 Facebook for Business, "Help Your Ads Find the People Who Will Love Your Business" <https://www.facebook.com/business/a/online-sales/ad-targeting-details> (accessed 5 November 2016).

21 Charles Duhigg, "How Companies Learn Your Secrets" *The New York Times* (16 February 2012).

22 Amy J Schmidtz & Colin Rule, *The New Handshake: Online Dispute Resolution and the Future of Consumer Protection* (American Bar Association, 2018) ch 4.

greater precision. Face2Gene, a facial recognition App, took advantage of the fact that people with genetic conditions (such as down syndrome) would sometimes exhibit a distinctive set of facial features.[23] The App developers trained their algorithms using a large database of photos of people with known diagnoses to find facial features that are associated with particular genetic conditions. Its findings can potentially be more reliable than even the most skilled human dysmorphologist, who can only see a limited number of patients in his lifetime. Similar techniques may be used to identify other diseases. For instance, researchers have used machine learning to help with early detection of autism in infants as well as Alzheimer's disease.[24]

14 Our voice data, on the other hand, may be used to train digital assistants, such as Amazon's Alexa and Apple's Siri,[25] to recognise and respond to our verbal requests to carry out a wide variety of tasks ranging from checking weather to ordering products online. It may even be used to train digital assistants to perform tasks that could previously only be performed by humans. Many people would probably remember a pre-recorded demo released by Google in 2018: Google's robot assistant, which sounded "eerily lifelike", called real people and successfully made appointments for a haircut and for lunch.[26]

III. Private, common and public property rights in personal data

A. Beyond data protection law

15 This article seeks to demonstrate that, in addition to data protection law, it is also helpful to examine personal data from a property law perspective. The reasons are multifold. First of all, as the bright side of the personal data story has shown, data has increasingly become a valuable resource. Since property law is essentially concerned with the allocation of valuable resources, it is well suited to address issues such as who should have access to and control over personal data, as well as the conditions for such access and control. In allocating control

23 Bonnie Rochman, "Diagnosing Disease with a Snapshot" *MIT Technology Review* (6 December 2016) <https://www.technologyreview.com/s/603038/diagnosing-disease-with-a-snapshot/> (accessed 10 December 2020).

24 Megan Molteni, "Thanks to AI, Computers Can Now See Your Health Problems" *Wired* (9 January 2017) <https://www.wired.com/2017/01/computers-can-tell-glance-youve-got-genetic-disorders/> (accessed 10 December 2020).

25 Brian X Chen, "Hi, Alexa. How Do I Stop You from Listening in on Me?" *The New York Times* (21 August 2019).

26 Olivia Solon, "Google's Robot Assistant Now Makes Eerily Lifelike Phone Calls for You" *The Guardian* (8 May 2018).

over a resource, property law takes into account a wide variety of values and interests, ranging from privacy,[27] desert,[28] self-development,[29] to incentivising investment in the creation of valuable resources.[30] Data protection law, on the other hand, appears to place greater emphasis on the dark side of the personal data story. The Personal Data Protection Act 2012[31] ("PDPA"), the principal data protection legislation in Singapore, applies only to "personal data", which is defined more narrowly as data that, either on its own or in combination with other data, can be used to identify one or more individuals.[32] In other words, the PDPA focuses on data practices that have the potential to undermine individual privacy. The starting point is to protect an individual's right to control his "personal data" (as defined) unless such right is outweighed by other countervailing considerations, such as the interest of an organisation, as well as the public, in collecting and using that data.[33]

16 In addition, property law is equipped with a diverse set of tools to balance this wide range of values and interests in allocating valuable resources. For example, it recognises multiple forms of property rights that a person may have in a resource,[34] which rights vary both in duration and in scope.[35] Property law also provides for various ways that different persons may access or benefit from the same resource (*eg*, through co-ownership or trust). By contrast, the main approach in data protection law for striking a balance between the interests of an individual and of society in personal data is to carve out exemptions from the requirement to seek an individual's consent before collecting and using his data. For example, personal data may be collected, used and disclosed without

27 Abraham Bell & Gideon Parchomovsky, "The Privacy Interest in Property" (2019) 167 U Pa L Rev 869.

28 John Locke & Peter Laslett, *Locke: Two Treatises of Government* (Student Edition) (Cambridge University Press, 1988).

29 Gregory S Alexander, *Property and Human Flourishing* (Oxford University Press, 2018).

30 See, *eg*, *GS Rasmussen & Associates, Inc v Kalitta Flying Service, Inc* 958 F 2d 896 (9th Cir, 1992).

31 Act 26 of 2012.

32 Personal Data Protection Act 2012 (Act 26 of 2012) s 2(1).

33 See, *eg*, s 3 of the Personal Data Protection Act 2012 (Act 26 of 2012). It recognises, after all, that a balance has to be struck between an individual's right to protect his personal data and the interest of an organisation, as well as the public, in collecting and using such data. The balance is mainly achieved by carving out exemptions from the requirement to seek individual consent. For example, personal data may be collected, used and disclosed without consent under various circumstances which are outlined respectively in the Second, Third and Fourth Schedules to the Personal Data Protection Act 2012.

34 Certain types of property rights may not be available in respect of some types of property. For example, one cannot have freehold over chattels.

35 For example, easement is more limited in scope than full ownership.

consent under various circumstances which are outlined in the Second, Third and Fourth Schedules to the PDPA. As such, property law may be able to provide a more diverse and nuanced approach to allocating access to and control over personal data.

B. Private, common and public property rights

17 Broadly speaking, there are three main types of property: private property, common property and public property. Much scholarly attention has been devoted to identifying the justifications for and the key elements of private property.[36] By contrast, the definitions of common and public property, as well as the relationship between private, common and public property, are less clear.

18 According to Jeremy Waldron, private property, common property and public property represent three systems of rules governing people's access to and control over resources.[37] In a private property system, individual asset owners determine who has access to their resources and how those resources shall be used; in a common property system, the community, through collective decision-making, determines how resources are to be used; finally, in a public property system, resources are accessible to all members of the society, subject only to restrictions that aim to secure fair access for all.[38]

19 Other scholars place greater emphasis on to whom access to a resource is granted. For example, Christopher Rodgers distinguishes private property rights from common and public property rights mainly based on the recipient of the right.[39] A private property right allows access to a resource to be controlled by the owner of that resource; a common property right grants access to the resource to a class of defined users; finally, a public property right provides the public with access to the resource.[40] A major consequence of this approach, Rodgers claims, is the

36 Christopher Rodgers, "Towards a Taxonomy for Public and Common Property" (2019) 78 Camb LJ 124.

37 Jeremy Waldron, "What Is Private Property?" (1985) 5 OxJLS 313. Waldron uses the terms private, collective and common property instead to refer to private, common and public property.

38 Jeremy Waldron, "Property and Ownership" in *Stanford Encyclopedia of Philosophy Archive* (Edward N Zalta ed) (Metaphysics Research Lab, Stanford University, 2020 Ed) <https://plato.stanford.edu/archives/sum2020/entries/property/> (accessed 9 July 2020).

39 Christopher Rodgers, "Towards a Taxonomy for Public and Common Property" (2019) 78 Camb LJ 124 at 130–132.

40 Christopher Rodgers, "Towards a Taxonomy for Public and Common Property" (2019) 78 Camb LJ 124.

recognition that private, common and public property rights can co-exist over the same resource.[41] In this respect, he shows how these three types of rights can co-exist in England using the example of common land: first of all, owners of common land enjoy various private property rights, such as the right to grant leases. The right to take produce of the common land, which is shared among a class of registered right holders, is a common property right. Lastly, the statutory right to access common land is enjoyed by the public at large and therefore a public property right.

20 Rodgers is not the first to observe that different property rights can exist in the same resource. In an earlier article, Henry Smith coined the term "semicommons", which refers to situations in which a resource is "owned and used in common for one major purpose, but, with respect to some other major purpose, individual economic units … have property rights to separate pieces of the commons".[42] The archetypical example of semicommons given by Smith is the open-field system of medieval and early modern northern Europe. In that system, peasants had private property rights to the produce they grew on their individual strips; under certain conditions, however, they were obligated to open their land to other landowners in the community for grazing.[43] According to Smith, semicommons is particularly suited for resources that can be used for multiple purposes while the efficient scale for one use differs from that of another. In the case of the open-field system, the efficient land size for grazing was much bigger than that for grain growing. In the case of personal data, the efficient scale for one use (*eg*, training algorithms) is also considerably bigger than that of another use (*eg*, protecting individual privacy). Moreover, with the appropriate protective measures in place, these different uses of personal data could be compatible with each other. As such, semicommons provides a useful framework for analysing rights relating to personal data.

IV. Private property rights in personal data

21 Adopting Rodgers' taxonomy, Parts IV[44] and V[45] of this article will consider the arguments for recognising both private and common property rights in personal data.

41 Christopher Rodgers, "Towards a Taxonomy for Public and Common Property" (2019) 78 Camb LJ 124 at 131.

42 Henry E Smith, "Semicommon Property Rights and Scattering in the Open Fields" (2000) 29 *The Journal of Legal Studies* 131 at 131.

43 Henry E Smith, "Semicommon Property Rights and Scattering in the Open Fields" (2000) 29 *The Journal of Legal Studies* 131 at 132.

44 See paras 21–53 below.

45 See paras 54–70 below.

A. Personal data is not private property under existing law

22 The idea of propertising personal data is often met with skepticism since the court has generally been reluctant to treat information as private property.[46] In *Boardman v Phipps*,[47] Lord Upjohn famously said: "In general, information is not property at all. It is normally open to all who have eyes to read and ears to hear." More recently, Floyd J observed that though information may give rise to intellectual property rights, "the law has been reluctant to treat information itself as property".[48] While certain types of personal data (*eg*, photos) are protected by copyright law,[49] a significant part of what we normally consider personal data (such as location data, browser history) is merely individual strands of information which is unlikely protected by copyright.[50]

23 Similarly, the traditional position under US law is that personal data cannot be owned by anyone.[51] There have been a number of unsuccessful attempts to claim property rights over personal data disclosed to service providers. For example, in *In re iPhone Application Litigation*,[52] the plaintiffs brought a class action against Apple, alleging that Apple's "iOS" operating systems unlawfully allowed third party applications to collect the plaintiffs' personal data (including user location, zip code and device identifier) without their consent.[53] The plaintiffs argued, among other things, that Apple was liable for conversion of their personal data.[54] However, the court ruled against the plaintiffs on the ground that their personal data did not constitute property.[55] Similarly, in *Low v LinkedIn Corp*,[56] the court, after noting that the weight of authority was against treating personal information as property, held that the plaintiffs did not

46 For a helpful discussion of the position at common law, see Lee Pey Woan, "Personal Data As a Proprietary Resource" in *AI, Data and Private Law: Translating Theory into Practice* (Gary Chan & Yip Man eds) (Hart Publishing, forthcoming).

47 [1967] 2 AC 46 at 127.

48 *Your Response Ltd v Datateam Business Media Ltd* [2015] QB 41 at [42]. Information may nevertheless give rise to database rights and copyright.

49 A detailed discussion of which types of personal data are copyrightable is outside the scope of this article since this article considers the question of whether personal data should be protected under general property law.

50 Law Reform Committee, Singapore Academy of Law, *Rethinking Database Rights and Data Ownership in an AI World* (July 2020) at para 3.22.

51 Pamela Samuelson, "Privacy As Intellectual Property" (2000) 52 Stan L Rev 1125 at 1131 ("the traditional view in American law has been that [personal data] cannot be owned by any person").

52 844 F Supp 2d 1040 (ND Cal, 2012).

53 *In re iPhone Application Litigation* 844 F Supp 2d 1040 at 1049 (ND Cal, 2012).

54 *In re iPhone Application Litigation* 844 F Supp 2d 1040 at 1074 (ND Cal, 2012).

55 *In re iPhone Application Litigation* 844 F Supp 2d 1040 at 1075 (ND Cal, 2012).

56 900 F Supp 2d 1010 (ND Cal, 2012).

have a property interest in the data disclosed by LinkedIn to third parties (which included users' LinkedIn ID and browsing history).

B. The exclusive right to commercialise personal data

24 Before examining the arguments in favour of propertising personal data, let us first consider what it means for an individual to own his data. The answer is far from clear for two reasons.

25 First, as Arnold Weinrib has noted, labelling something as private property does not define the scope or the content of its owner's rights.[57] Under one view, the essential feature of property rights is the right to exclude. According to James Penner, a well-known proponent of this view, ownership of tangibles has a core tripartite structure, including (a) the right to immediate, exclusive possession; (b) the power to license others to take possession; and (c) the power to dispose of one's title.[58] Ownership of intangibles, on the other hand, is "inherently exclusive" since a third party cannot do anything to extinguish this right in normal circumstances.[59] Another view of property rights is that each owner has a "bundle of rights" over his property, which bundle does not have any core structure. In other words, the content and scope of an owner's bundle of rights is mostly dictated by public policy considerations in specific cases.[60] There have been many attempts to elaborate on what that bundle consists of. An oft-cited list is the 11 "standard incidents of ownership" proposed by Tony Honore, which include the right to use, the right to manage, the right to the income of the thing, the right to the capital, the right to security, the rights of transmissibility and absence of term, the prohibition of harmful use, liability to execution, and the incident of residuarity.[61] A person need not possess all 11 incidents to be considered the owner of a resource.

26 Second, at first glance, certain features of personal data do not seem to sit comfortably with the idea of ownership. To begin with, personal data is non-rivalrous, that is, possession and use of a piece of

57 Arnold S Weinrib, "Information and Property" (1988) 38 *University of Toronto Law Journal* 117 at 120.

58 J E Penner, *Property Rights: A Re-Examination* (Oxford University Press, 2020) at p 40.

59 J E Penner, *Property Rights: A Re-Examination* (Oxford University Press, 2020) at p 42.

60 See J E Penner, *Property Rights: A Re-Examination* (Oxford University Press, 2020) ch 3.

61 See, *eg*, A M Honoré, "Ownership" in *Oxford Essays in Jurisprudence: A Collaborative Work* (Anthony G Guest ed) (Oxford University Press, 1961). These incidents are not individual necessary conditions of ownership.

data by one person does not prevent another person from possessing or using the same data. Moreover, a piece of data can often be copied easily and at a relatively low cost. As a result, it is often difficult for a person to exclude others from accessing his personal data. Consider the simple example of meeting someone for lunch. Your location data would likely be disclosed not only to your friend but also your cellphone service provider, Google/Apple (or any other mobile Apps with access to your location data), and indeed every other person who happens to be at the restaurant at the same time as you. It would not be practically possible (or desirable) to force all of them to forget the fact that you were in the restaurant or not to mention it without seeking your consent. The only way to have exclusive control over one's location data would probably be to remain alone and shut down all access to the outside world.

27 In addition to the practical difficulty of excluding access to personal data, it is also questionable whether an individual should be granted the right to exclude such access in the first place. Carol Rose argues that certain things are inherently public for two related reasons: firstly, they are more valuable when they are accessible to the public; secondly, the public deserve access to these things because their value is created by the public.[62] Examples of such inherently public things include commerce, education, good manners, recreation, free speech, and so on.[63] These things often produce desirable values: for example, they may act as social glues or promote democracy.[64] One may argue that certain types of personal data, such as people's names, are inherently public since such information is more valuable when it is accessible to other people. There is arguably little point in having a name unless other people know about and use it.

28 A related concern is that having private property rights in personal data may allow an individual to prevent others from disclosing certain information relating to him even where such disclosure is desirable.[65] For example, if an individual is granted exclusive control over his geo-location data, he can presumably prevent a journalist from reporting his appearance in an illegal drug den even if that information

62 Carol Rose, "The Comedy of the Commons: Custom, Commerce, and Inherently Public Property" (1986) 53(3) U Chi L Rev 711 at 769–770.

63 Carol Rose, "The Comedy of the Commons: Custom, Commerce, and Inherently Public Property" (1986) 53(3) U Chi L Rev 711 at 776–777.

64 Carol Rose, "The Comedy of the Commons: Custom, Commerce, and Inherently Public Property" (1986) 53(3) U Chi L Rev 711 at 778–779.

65 Jessica Litman, "Information Privacy/Information Property" (2000) 52 Stan L Rev 1283.

is newsworthy. Indeed, an oft-cited argument against propertising information is the public interest in the free flow of information.[66]

29 However, the foregoing concerns also apply to other types of intangible property and arguably should not, of themselves, present insurmountable obstacles to treating personal data as private property. First of all, an owner's right to exclude may be expressly created and protected by legislation, which is the case for various types of "regulatory property"[67] such as a right to emit carbon dioxide.[68] Moreover, one way to strike a balance between private and public interests in personal data is to provide for a weaker form of excludability.[69] This may be achieved either by narrowly defining the subject matter of the property right or by narrowly defining the right itself. An example of the former approach would be copyright, which protects only expressions, not ideas;[70] an example of the latter approach can be found in the right of publicity, which only applies to commercial use of one's identity.[71]

30 In the case of personal data, it is envisaged that propertising personal data would not provide an individual with an absolute right to exclude everyone from accessing his personal data. Rather, he would only enjoy the exclusive right to commercialise his data. Certain practices, such as granting access to one's data in exchange for monetary returns or using personal data to develop commercial products, would likely fall within the scope of "commercialising" personal data. This article does not, however, seek to provide a comprehensive definition of commercialising personal data; whether an activity amounts to commercialising personal data is better to be decided on a case-by-case basis.

66 See, *eg*, *R v Stewart* [1988] 1 SCR 963 (SCC).

67 The phrase has been used to refer to a property right "created and allocated by a government entity". Bruce Yandle & Andrew P Morriss, "The Technologies of Property Rights: Choice among Alternative Solutions to Tragedies of the Commons" (2001) 28(1) *Ecology Law Quarterly* 123 at 129.

68 Carbon emissions allowance was held to be a form of "other intangible property" in *Armstrong v Winnington* [2013] Ch 156; [2012] EWHC 10 (Ch).

69 See, *eg*, Tanya Aplin, "Confidential Information as Property?" (2013) 24 King's LJ 172 at 194.

70 See, *eg*, Art 9(2) of the TRIPS Agreement, which provides that copyright protection extends to "expressions, and not to ideas, procedures, methods of operation or mathematical concepts".

71 See, *eg*, David Tan, "Affective Transfer and the Appropriation of Commercial Value: A Cultural Analysis of the Right of Publicity Entertainment" (2010) 9 *Virginia Sports and Entertainment Law Journal* 272 at 273.

C. Grounds for granting private property rights in personal data

(1) To bolster individuals' control over their personal data

31 To a certain extent, an individual already enjoys some right to exclude others from the personal data about him under existing law. While the PDPA is not intended to confer any property rights over personal data to any individual or organisation, it has rendered personal data "excludable" in many situations. The PDPA requires an organisation to obtain an individual's consent before collecting, using or disclosing personal data about him and to inform the individual of the purpose for such collection, use or disclosure.[72] According to one leading commentator, the PDPA has laid down a framework that is conducive to the development of property rights in personal data by conferring rights of control on data subjects.[73]

32 Treating individuals as owners of their personal data has potential to provide them with greater control over their data. To begin with, the right to exclude collection and use of personal data under the PDPA does not apply to certain exempt persons[74] (including any individual acting in a personal or domestic capacity and any public agency) and exempt circumstances.[75] By contrast, an individual's exclusive right to commercialise his personal data is *prima facie* wide enough to exclude all non-owners from collecting and using his personal data for commercial purposes. Moreover, the PDPA arguably does not apply to personal data about an individual who has been dead for more than ten years.[76] Treating personal data as private property, on the other hand, raises the possibility of inheriting personal data and controlling such data for a considerably longer period of time.

33 Additionally, while s 32 of the PDPA provides for a private right of action to seek relief for loss suffered as a result of a contravention of the PDPA, this right to seek relief appears to be limited in two ways. First, it might not allow an individual to seek relief from a hacker who acts in

72 Personal Data Protection Act 2012 (Act 26 of 2012) ss 13 and 20.

73 Lee Pey Woan, "Personal Data as a Proprietary Resource" in *AI, Data and Private Law: Translating Theory into Practice* (Gary Chan & Yip Man eds) (Hart Publishing, forthcoming).

74 Personal Data Protection Act 2012 (Act 26 of 2012) s 4(1).

75 See the Second, Third and Fourth Schedules to the Personal Data Protection Act 2012 (Act 26 of 2012).

76 It only applies to a limited extent to personal data about an individual who has been dead for ten years or less. Personal Data Protection Act 2012 (Act 26 of 2012) s 4(4). Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (23 September 2013; revised 2 June 2020) at paras 5.19 and 5.20.

a personal capacity. Second, it may not allow an organisation to obtain relief for contraventions of the PDPA. In a recent District Court decision, *IP Investment Management Pte Ltd v Alex Bellingham*,[77] the court held that the right of action under s 32 was available only to individual data subjects or organisations acting on their behalf, as opposed to organisations in general.[78] As explained more fully in the following subsection, treating personal data as private property can potentially allow an organisation to bring an action against persons who misappropriate personal data held by that organisation on the basis that it interferes with its proprietary interest over that data. If so, it would provide additional incentives for an organisation to safeguard the personal data under its control.

34 Finally, it is worth noting that treating personal data as private property does not resolve all the problems relating to the collection and use of personal data outlined above.[79] An individual's control over his personal data is still likely to be undermined in several ways. For example, service providers generally have strong incentives to seek permission to use personal data for a wide variety of purposes; at the same time, an individual often lacks the bargaining power to negotiate more favourable terms with those service providers. Moreover, since personal data can be used in many unforeseeable ways, it is hard for an individual to decide in advance which use should be permitted; this difficulty is compounded by the fact that data can potentially be copied and passed on to countless third parties. Further, an individual is likely to have little time and resources to verify whether a data collector uses his data in ways that conform to his preferences or to take enforcement actions against data collectors/users when they fail to do so.

(2) Provide additional incentives to secure personal data

35 If personal data were considered private property, then it is possible to treat an organisation as having a possessory interest in the personal data that it has lawfully acquired from the owner of that data. If we choose to recognise such a possessory interest, then according to the principle of relativity of title, which is an essential feature of property law, the organisation would acquire a "title" to that personal data, which is enforceable against all third parties who cannot prove a stronger title.

36 An organisation may then be entitled to bring an action against persons that interfere with its possessory interest in that personal data (for example, by misappropriating such data through hacking). The ability

77 [2019] SGDC 207 at [110].
78 The correctness of the court's decision is debatable.
79 See paras 5–10 above.

to seek relief from such persons is likely to provide greater incentives for an organisation to investigate and locate wrongdoers that collect and use personal data without the requisite consent. To the extent that the threat of litigation has some deterrent effect on potential wrongdoers, it provides individual data subjects with some additional protection, however limited, over their data.

37 Nevertheless, there has been some controversy over whether data, which is intangible, can be possessed. The traditional view is that intangible things cannot be possessed, which has been affirmed in the English Court of Appeal case of *Your Response Ltd v Datateam Business Media Ltd*.[80] In that case, the plaintiff sought to assert a lien over a database in digital form, which raised the question of whether it was possible to have actual possession of an intangible thing.[81] The court answered the question in the negative, rejecting the plaintiff's argument that possession should be equated with practical control. According to the court, possession was concerned with "physical control of tangible objects", while practical control was a broader concept which could extend to both intangible property and non-property.[82] However, it is not inconceivable to expand the notion of possession from physical control to practical control. Some US courts have indeed taken the step to allow possession of intangible things. In *Thyroff v Nationwide Mutual Insurance Co*,[83] the court noted that information often had intrinsic value regardless of whether the format in which the information was stored was tangible or intangible. As such, the court held that electronic records that were stored on a computer should not be treated differently from printed documents and accordingly should be subject to a claim in conversion.

(3) To reduce misuse of personal data

38 There are two related problems with the way personal data is currently used. First, a data collector often has an incentive to collect and use as much personal data as possible. As a result, an individual whose data has been collected receives an increasing number of messages from both advertisers and potential fraudsters. In turn, he is likely to pay less attention to each message received, thereby reducing the return each user can get from his data. This tendency to overuse personal data can be explained by the tragedy of the commons phenomenon.[84] An

80 [2015] QB 41.
81 *Your Response Ltd v Datateam Business Media Ltd* [2015] QB 41 at [12].
82 *Your Response Ltd v Datateam Business Media Ltd* [2015] QB 41 at [23].
83 8 NY 3d 283 at 292–293 (2007).
84 Garrett Hardin, "The Tragedy of the Commons" (1968) 162 *Science* 1243.

oft-prescribed solution to this problem is to create property rights over the resource that is being overused.

39 Another problem, which has been outlined above,[85] is that an individual may suffer physical, emotional or financial harm as a result of the collection and use of his data. However, since the harm is mainly suffered by the individual, rather than the person using his data, data users have little incentive to refrain from collecting and using that individual's data. In other words, data users often do not internalise the externalities that they impose on others. A common solution to this problem is to require the creator of those externalities to internalise them (*eg*, by paying for them).

40 In light of these problems, various scholars have suggested giving individuals property rights over their data, which allows them to sell that data.[86] A familiar line of argument in favour of a market-based approach to personal data goes as follows: an individual has the greatest incentive to maximise the value of his personal data; having property rights in his data will sometimes help him prevent others from misusing his data, thereby alleviating the tragedy of the commons problem. Moreover, an individual is also in the best position to determine the value of his data; having property rights in that data will enable him, either directly or through agents, to sell it to data collectors at a mutually agreeable price. In the meantime, as data collectors and users are forced to "internalise" the costs of collecting and using personal data, they are likely to collect and use less data.[87]

(4) To incentivise transfer of personal data for socially beneficial purposes

41 A classic utilitarian argument in favour of granting the right to exclusive control over a thing runs as follows: such a right provides strong incentives to the right holder to invest his time and resources in that thing because he is able to reap the full benefit of it. The typical argument for granting intellectual property rights, such as copyright and patent, falls within this utilitarian tradition: without such exclusive rights, it is suggested, people would be less likely to invest time and energy into producing creative expressions and innovative works due to the free-

85 See paras 9–10 above.

86 See, *eg*, Kenneth C Laudon, "Markets and Privacy" (1996) 39(9) *Communications of the ACM* 92; and Richard S Murphy, "Property Rights in Personal Information: An Economic Defense of Privacy" (1995) 84 Geo LJ 2381.

87 Pamela Samuelson, "Privacy as Intellectual Property" (2000) 52 Stan L Rev 1125 at 1133.

rider problem;[88] inventors will have greater incentives to hide the details of their inventions from the public, thereby reducing the likelihood that others will benefit from that knowledge.

42 In a similar vein, granting individuals the exclusive right to commercialise their personal data would likely provide additional incentives for them to contribute their data for socially beneficial purposes. It has been suggested that trust in both researchers and research institutions is a "necessary prerequisite for participating in research".[89] A failure to provide individuals with adequate control and compensation for their data might lead to concerns about exploitation as well as distrust of researchers.[90] Some scholars fear that people might simply "take their data and go home" instead of taking part in research that could generate socially beneficial knowledge.[91] On the other hand, an individual is likely to be more willing to share his personal data if he receives proper remuneration for it.[92] Indeed, several companies have sought to create a platform through which people are compensated for sharing their genetic data with researchers.[93]

D. Concerns over granting private property rights in personal data

(1) Difficulty in policing data resellers

43 One key obstacle to establishing a market through which individuals can sell their personal data is the fact that personal data is non-rivalrous and can be easily copied and sold by whoever is in possession of such data. As a result, even if an individual has the right to exclude others from his data, he is unlikely to be able to get the full price for his data if a buyer is capable of undercutting his market share (*eg*, by selling his data at a cheaper price). As a result, an individual might not have sufficient incentives to sell his data in the first place; nor would a data

88 See, *eg*, *GS Rasmussen & Associates, Inc v Kalitta Flying Service, Inc* 958 F 2d 896 at 903 (9th Cir, 1992).

89 Jessica L Roberts, "Progressive Genetic Ownership" (2018) 93 Notre Dame L Rev 1105 at 1135.

90 Jessica L Roberts, "Progressive Genetic Ownership" (2018) 93 Notre Dame L Rev 1105 at 1135.

91 Barbara J Evans, "Barbarians at the Gate: Consumer-Driven Health Data Commons and the Transformation of Citizen Science" (2016) 42 *American Journal of Law & Medicine* 651 at 658.

92 Jessica L Roberts, "Progressive Genetic Ownership" (2018) 93 Notre Dame L Rev 1105 at 1137 (one possible explanation provided by DNA simple's CEO is that people "feel [like] part of the process when they get compensated").

93 Jessica L Roberts, "Progressive Genetic Ownership" (2018) 93 Notre Dame L Rev 1105 at 1137.

user be incentivised to purchase from that individual if it can obtain the same data elsewhere at a lower cost.

44 This excludability problem is partially alleviated by restrictions on transfer of data under existing law. For example, the PDPA requires an organisation to obtain consent from a data subject before using or disclosing "personal data" about him.[94] Further restrictions may be imposed by contract. For example, Pamela Samuelson has proposed a data licensing regime that requires a sub-licensee to comply with the same conditions that have been imposed on the relevant sub-licensor.[95] Similarly, Woodrow Hartzog has argued for a "chain-link confidentiality approach" that uses contracts to impose obligations on third-party recipients of data.[96]

45 Property law could provide additional conceptual tools to address this excludability problem. For example, a classic principle of land law provides that the benefits and burdens of a covenant can "run with the land" if certain conditions are satisfied.[97] A modified version of this principle could provide that certain obligations, such as a duty to provide compensation for the commercial use of personal data, contained in a contract between an individual and a data collector should "run with the data". As a result, any person receiving that data from the data collector would be bound by the same obligation.

(2) Undermines dignitary interests

46 Another objection against propertising personal data is the belief that it is inappropriate for individuals to own certain types of data.[98] For example, Sonia Suter claims that treating medical information as property "distorts and impoverishes our understanding of the dignitary [and] personhood interests we have in this information".[99]

94 Personal Data Protection Act 2012 (Act 26 of 2012) s 13.

95 Pamela Samuelson, "Privacy as Intellectual Property" (2000) 52 Stan L Rev 1125 at 1158.

96 Woodrow Hartzog, "Chain-Link Confidentiality" (2012) 46 Ga L Rev 657 at 661. These contracts will include terms which (a) impose obligations on a data recipient to use it in a particular manner; (b) require that recipient to bind future recipients to the same obligations; and (c) require those future recipients to impose the same confidentiality terms on subsequent recipients.

97 Tang Hang Wu & Kelvin F K Low, *Tan Sook Yee's Principles of Singapore Land Law* (LexisNexis, 3rd Ed, 2009) ch 17.

98 See, *eg*, Julie E Cohen, "Examined Lives: Informational Privacy and the Subject as Object" (2000) 52 Stan L Rev 1373 at 1378.

99 Sonia M Suter, "Disentangling Privacy from Property: Toward a Deeper Understanding of Genetic Privacy" (2004) 72 Geo Wash L Rev 737.

47 However, reasonable minds are likely to disagree as to whether respect for human dignity militates against recognising property interests in personal data. For example, in *Moore v Regents of University of California*,[100] the judges of the Supreme Court of California expressed drastically different views as to whether allowing an individual to assert ownership over cells which were removed from his body would protect or undermine human dignity. Arabian J characterised the plaintiff's attempt to claim property rights in his cells as an invitation to "enforce a right to sell one's own body tissue for profit" and was appalled by the thought.[101] According to him, equating human tissue with a commercial commodity would "commingle the sacred with the profane".[102] Mosk J, however, was of the view that one manifestation of our respect for the human body is the prohibition against "indirect abuse of the body by its economic exploitation for the sole benefit of another person".[103] Failing to recognise property interest in human tissue would result in exactly that – it allows researchers to use a patient's tissue as a means to an economic end.[104]

48 Moreover, the personhood theory of property law may in fact support treating personal data as private property. According to Margaret Radin, a champion of the personhood theory, we should draw a distinction between personal things and fungible ones.[105] Personal things are those that people "feel are almost part of themselves"; fungible things are perfectly replaceable.[106] Radin maintains that greater control should be accorded to personal things: if a thing is so bound up with one's person, the need to control it may be akin to the need to protect one's bodily integrity.

49 It is arguable that at least certain types of personal data would fall within the category of "personal things". For example, an individual's Facebook profile and activities over an extended period of time may form an integral part of the virtual image that he carefully chooses to present to outsiders. Additionally, one may argue that such data is literally constitutive of himself since it can reveal so much of his personal characteristics, personality and preferences. As noted above,[107] information such as Facebook "likes" can be used to predict a wide range of personal attributes, including ethnicity (95% accuracy), sexual

100 *Moore v Regents of University of California* 51 Cal 3d 120 (1990).
101 *Moore v Regents of University of California* 51 Cal 3d 120 at 148 (1990).
102 *Moore v Regents of University of California* 51 Cal 3d 120 at 149 (1990).
103 *Moore v Regents of University of California* 51 Cal 3d 120 at 173 (1990).
104 *Moore v Regents of University of California* 51 Cal 3d 120 at 174 (1990).
105 Margaret Jane Radin, "Property and Personhood" (1981) 34 Stan L Rev 957 at 959–961.
106 Margaret Jane Radin, "Property and Personhood" (1981) 34 Stan L Rev 957 at 961.
107 See para 8 above.

orientation (88% accuracy for males and 75% for females), Democrats and Republicans (85% accuracy), and substance use (between 65% and 75% accuracy).[108] As a result, an analysis of an individual's personal data can sometimes be as intrusive as (if not more intrusive than) a bodily search. Where the relevant personal data is so closely connected with an individual's personhood, it arguably deserves heightened protection under property law.

(3) The anti-commons problem

50 The tragedy of the anti-commons, which is a mirror image of the more familiar tragedy of the commons, occurs where a resource is underused because too many people have a right to exclude others from using it.[109] As Lee Anne Fennel has observed, anti-commons has become a shorthand for problems with assembling entitlements. The main concern is that a value-enhancing assembly "will fail to occur as a result of strategic holdout behavior and other transaction costs".[110]

51 In the case of personal data, one may argue that if individuals had property rights over their personal data, then a data collector and/or data user would be required to negotiate with every individual whose data it intends to collect or use. The costs involved in obtaining multitudinous consents would be so high as to prevent, in at least some instances, socially beneficial use of such data. Two types of costs are particularly relevant. First, the costs involved in establishing the necessary infrastructure to facilitate the exchange of personal data. For example, Kenneth Laudon proposes that we create a "National Information Market" through which each individual can sell his data.[111] The costs of creating such a property system will likely be significant.[112] Second, the total costs involved in getting permission from each individual to use his data may also be high. The cost would likely be higher if some individuals intentionally hold out, that is, refusing to give permission in the hope of receiving higher compensation for the data in their possession.

108 Michal Kosinski, David Stillwell & Thore Graepel, "Private Traits and Attributes Are Predictable From Digital Records of Human Behavior" (2013) 110(15) *Proceedings of the National Academy of Sciences* 5802.

109 See Michael A Heller, "The Tragedy of the Anticommons: Property in the Transition from Marx to Markets" (1998) 111 Harv L Rev 621.

110 Lee AnneFennell, "Commons, Anticommons, Semicommons" in *Research Handbook on the Economics of Property Law* (Kenneth Ayotte & Henry E Smith eds) (Edward Elgar Publishing, 2011) at p 41.

111 See Kenneth C Laudon, "Markets and Privacy" (1996) 39(9) *Communications of the ACM* 92.

112 Pamela Samuelson, "Privacy As Intellectual Property" (2000) 52 Stan L Rev 1125 at 1137.

52 Nevertheless, it is submitted that providing individuals with the exclusive right to commercialise their data is unlikely to raise serious anti-commons concerns for two main reasons. First, an individual often has limited power to exercise his right to exclude data collectors. This is sometimes because he is unaware that his personal data is being collected or used.[113] Although many service providers explain when and how they collect personal data in their privacy policies, several empirical studies indicate that people seldom read those policies.[114] Even if an individual is aware that his personal data is being collected, he may not have a choice whether to allow such collection. Social media has increasingly become an integral part of people's lives. Once an individual decides to maintain a social media profile, which an estimated 3.8 billion people do,[115] he would often have no choice but to share his personal data with social media companies such as Facebook and Twitter. Second, personal data about an individual is often substitutable from a data user's perspective. For example, a company seeking to identify characteristics that are predictive of a person's likelihood to repay his loan does not need data from every borrower. Consequently, an individual would less likely be able to receive significantly greater compensation for his data by holding out.[116]

53 By contrast, the anti-commons problem would be more pronounced in the case of personal data held by companies. As explained more fully in Part V below, a company often has significant incentives to exclude others from accessing the personal data in its possession; such data is also more likely to be unique (in other words, less substitutable). As a result, there is a stronger argument for granting common property rights over such data.

113 See, *eg*, Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (Random House, 2001).

114 See, *eg*, Ryan Calo, "The Boundaries of Privacy Harm" (2011) 86 Ind LJ 1131; and Ian Ayres & Alan Schwartz, "The No-Reading Problem in Consumer Contract Law" (2014) 66 Stan L Rev 545.

115 An estimated 3.8 billion people are active social media users: John Koetsier, "Why 2020 Is a Critical Global Tipping Point for Social Media" *Forbes* (18 February 2020).

116 Thanks to Prof Daniel Seng for raising the point that we might need everybody's data in public health emergencies. Presumably using personal data to prevent a public health crisis would not fall within the definition of "commercialising personal data".

V. Common property rights in personal data

A. De facto *control over personal data*

54 At the moment, companies such as Google and Facebook tend to opt for the following arrangement with their users: on the one hand, they claim that their users own the intellectual property rights (if any) in the data they provide to those service providers; on the other hand, they seek from their users a worldwide licence to use that data in virtually any way they want for free. For example, Facebook's terms of service provide that Facebook enjoys the right to "host, use, distribute, modify, run, copy, publicly perform or display, translate, and create derivative works of" any data provided by its users.[117] Similarly, Google seeks a licence from its users to use their data not only to operate and improve Google's existing services, but also to develop new technologies and services.[118]

55 While personal data is not the private property of individual data subjects, it appears increasingly like *de facto* "private property" of companies that collect and use such data.[119] A company in possession of a database of personal data is often able to take various measures to exclude others from accessing that database, including controlling access to the database through strong passwords, protecting the database against attacks using firewalls and encryption, and controlling access to the hardware on which the data is stored.

56 Moreover, the content of a database of personal data is often unique for a number of reasons. Firstly, much personal data is recorded while an individual interacts with a company's products and services, which are often unique to each company. For example, if an individual, say Mary, buys a dress from Amazon, only a handful of people, such as Mary's friends, would know of the purchase. Even fewer would know the exact time, location and price at which the dress is purchased. After several weeks, even Mary herself would have difficulty remembering such details without checking the shopping history kept by Amazon. Indeed, Amazon is likely to be the only party with a detailed record of Mary's purchase with Amazon over an extended period of time.

---

117 See, *eg*, Facebook, "Terms of Service" <https://www.facebook.com/terms.php> (accessed 12 April 2020).

118 Google, "Terms of Service" <https://policies.google.com/terms?hl=en-US> (accessed 12 April 2020).

119 See, *eg*, Lee Pey Woan, "Personal Data as a Proprietary Resource" in *AI, Data and Private Law: Translating Theory into Practice* (Gary Chan & Yip Man eds) (Hart Publishing, forthcoming); Nadezhda Purtova, "The Illusion of Personal Data as No One's Property" (2015) 7 *Law, Innovation and Technology* 83 at 84.

57 Secondly, behavioural data such as a person's purchase history is periodically updated. Each update might generate additional insights about the person to whom that data relates. As such, the company with access to the most comprehensive and up-to-date data has a distinct advantage. For example, Target was able to predict a girl's pregnancy from her shopping history even before her family were aware of it.[120] Another company with less up-to-date information on the girl probably would not be able to capitalise on such insights as well as Target.[121] Thirdly, as in the case of Target, a company is often able to infer additional information about its clients from the data it has collected. The content of such inferred data would depend largely on the company's ability and skill to process the data in its possession. Finally, a company often has a unique pool of clients, whose data may not be captured by a rival business.

58 Having access and control over a unique, valuable database provides a company with significant competitive advantage over its rivals. It is almost cliché to claim that data is the "new oil". From a company's perspective, this data can be valuable in a number of ways.

59 First, it enables a company to better serve the needs of its customers, thereby gaining an edge over its competitors at acquiring and retaining clients. For example, Netflix is able to use data ranging from user location, watch history, user interests and search words to provide personalised recommendations to its subscribers.[122] Second, it enables a company to more accurately price its products to different customers to maximise its profit. The Staples website allegedly displayed different prices to different online shoppers based on their locations and, in particular, their distance from a rival store (such as Office Depot).[123] Third, it enables a company to generate income by providing tailored advertisements to their customers: the more data a company has, the more targeted the audience, and more attractive the company is to advertisers. Companies such as Google and Facebook derive a large part of their revenue from advertising.[124] To this end, they make extensive use of user information.

120 Charles Duhigg, "How Companies Learn Your Secrets" *The New York Times* (16 February 2012).

121 By contrast, the quality and value of other, more static, types of personal data, such as one's name and genetic data, would not deteriorate as quickly over time.

122 Srivatsa Maddodi & Krishna Prasad K, "Netflix Bigdata Analytics – The Emergence of Data Driven Recommendation" (2019) 3(2) *International Journal of Case Studies in Business, IT, and Education* 41.

123 Jennifer Valentino-DeVries, Jeremy Singer-Vine & Ashkan Soltani, "Websites Vary Prices, Deals Based on Users' Information" *The Wall Street Journal* (24 December 2012).

124 See, *eg*, Trefis Team, "Google Q1 Earnings: Ad Revenues Post Growth Once Again" *Forbes* (27 April 2015); and Mike Isaac, "Facebook Revenue Surges 41%, As Mobile Advertising and Users Keep Growing" *The New York Times* (4 November 2015).

Google analyses user data (such as search terms and location) to serve ads and to measure the effectiveness of its advertising.[125] Facebook used user names and pictures to endorse products to their friends (which resulted in a class action brought against Facebook on the ground that its "Sponsored Stories" misappropriated users' names and likenesses).[126] Even traditional businesses have not missed the opportunity to cash in on their customer data. Banks reportedly make money out of their customer's shopping habits: they help retailers send targeted discounts to certain customers and get a percentage commission each time a customer makes a purchase.[127]

B. Multiple use of personal data

60 While a company can use the personal data it has collected to maximise its profit, the same data can often be used to further other goals and objectives.

61 A number of initiatives undertaken by technological companies have demonstrated how the wealth of personal data controlled by these companies might be used to help improve public welfare. More than a decade ago, Google researchers sought to improve early detection of seasonal influenza by monitoring flu-related search queries on Google.[128] The main idea was that people would be more likely to search for flu-related information when they were sick, thereby providing almost instant report of influenza epidemics in areas with a large number of web search users. While Google's flu-tracking service did not perform as well as expected, it does not detract from the fact that data held by companies has potential to be a valuable force for good.[129] More recently, Facebook's Disaster Map project uses aggregate data about Facebook usage in areas affected by natural disasters to create a series of maps which show the location and movements of Facebook users as well as where they charge and use their mobile phones.[130] These maps are intended to provide

125 Google, "Privacy & Terms: How Google Uses Information from Sites or Apps That Use Our Services" <https://policies.google.com/technologies/partner-sites?hl=en-US> (accessed 4 August 2020).

126 See, *eg*, *Fraley v Facebook, Inc* 830 F Supp 2d 785 (ND Cal, 2011).

127 Blake Ellis, "The Banks' Billion-Dollar Idea" *CNN Money* (8 July 2011).

128 Jeremy Ginsberg *et al*, "Detecting Influenza Epidemics Using Search Engine Query Data" (2009) 457 *Nature* 1012.

129 David Lazer & Ryan Kennedy, "What We Can Learn from the Epic Failure of Google Flu Trends" *Wired* (1 October 2015) <https://www.wired.com/2015/10/can-learn-epic-failure-google-flu-trends/> (accessed 20 July 2020).

130 Paige Maas *et al*, "Facebook Disaster Maps: Aggregate Insights for Crisis Response & Recovery" *Facebook Research* (19 May 2019) <https://research.fb.com/publications/facebook-disaster-maps-aggregate-insights-for-crisis-response-recovery/> (accessed 20 July 2020).

critical information to humanitarian organisations to enhance their relief efforts.[131] In a report entitled "The Potential of Social Media Intelligence to Improve People's Lives",[132] Stefaan Verhulst and Andrew Young provide a useful overview of how data held by social media companies can be used for the public good. Such data has, for example, been used to help predict floods, track anti-vaccination sentiments, provide insights on the impact of the Zika virus, detect adverse drug reactions, assess public engagement with climate change, and so on.

C. Grounds for granting common property rights in personal data

(1) To promote efficient use of data

62 Since data is non-rivalrous in consumption, the same dataset can in theory be used by multiple parties at the same time. It is not uncommon for a company to enter into an agreement to share its data with other companies. For example, Facebook reportedly had arrangements with more than 150 companies, including Microsoft, Amazon and Spotify, granting them special access to its user data.[133]

63 However, a company may be reluctant to share the data in its possession for various reasons. To begin with, data sharing might result in the disclosure of personally identifiable information. If it does, a company would be required to either seek prior consent from each individual affected by the disclosure or take steps to anonymise the data it intends to share. Both approaches have their associated costs. Firstly, taking steps to obtain informed consent to share personal data could be costly. While a company may disclose its intention to share user data in its privacy policy, such disclosure might not be adequate since many people do not read or understand privacy policies.[134] A company may opt for more effective (and likely more intrusive) ways to obtain informed consent. It can, in theory, require each prospective customer to take a quiz on when and how the company discloses user data. However,

131 "Disaster Maps" *Facebook Data for Good* <https://dataforgood.fb.com/tools/disaster-maps/> (accessed 20 July 2020).

132 Stefaan Verhulst & Andrew Young, "The Potential of Social Media – Intelligence to Improve People's Lives: Social Media Data for Good" *GovLab* (24 September 2017) <https://datacollaboratives.org/static/files/social-media-data.pdf> (accessed 20 July 2020).

133 Gabriel J X Dance, Michael LaForgia & Nicholas Confessore, "As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants" *The New York Times* (18 December 2018).

134 See, *eg*, Ryan Calo, "The Boundaries of Privacy Harm" (2011) 86 Ind LJ 1131; and Ian Ayres & Alan Schwartz, "The No-Reading Problem in Consumer Contract Law" (2014) 66 Stan L Rev 545.

these additional steps would likely involve greater administrative costs and may also result in a decline in user experience. The second approach, taking steps to anonymise personal data, is only available to companies with the requisite technical skills. Moreover, anonymisation not only takes time and effort, but is not foolproof. For example, part of an anonymised dataset released by Netflix in a contest to improve its recommendation system was subsequently re-identified by comparing it with public information in the Internet Movie Database, which led to a lawsuit brought against Netflix.[135]

64 In addition to concerns over privacy and security, a company may also decline to share data to protect its competitive advantage over its rivals. For example, Facebook reportedly "tracked the growth of competitors and denied them access to user data available to others".[136] Moreover, since data can often be copied, shared, and used for various purposes, there is a risk that the shared data might subsequently be used in ways that are detrimental to the company's interest. Even if a company has imposed various contractual restrictions and obligations on a data recipient, it nevertheless has to incur costs in monitoring the latter's compliance with the contract.

65 In light of the foregoing, there is sometimes a divergence in interest between an organisational data holder and the general public. While a company may not consider it cost-effective to share the personal data in its possession, the public might significantly benefit if that data were more widely accessible.

66 One way to strike a balance between a company's private interest and the public interest is to recognise limited common property rights in the dataset held by the company. The proposed right would specify the circumstances and conditions under which a company would be obligated to provide access to the data in its possession. For example, access rights may be granted only to parties that demonstrate the intention and ability to use the dataset for public purposes. Since such public uses are more likely to be compatible with a company's private uses of the same data, it would be less likely for data sharing to be a zero-sum game. Moreover, it would preserve the company's power to determine the use of the data in its possession in other situations. As a result, there is a lower risk that

135 Bruce Schneier, "Why 'Anonymous' Data Sometimes Isn't" *Wired* (12 December 2007) <https://www.wired.com/2007/12/why-anonymous-data-sometimes-isnt/> (accessed 21 July 2020); Ryan Singel, "Netflix Spilled Your Brokeback Mountain Secret, Lawsuit Claims" *Wired* (17 December 2009) <https://www.wired.com/2009/12/netflix-privacy-lawsuit/> (accessed 21 July 2020).

136 Paresh Dave & Munsif Vengattil, "Facebook Gave Data on User's Friends to Certain Companies: Documents" *Reuters* (5 December 2018).

a company would be discouraged from collecting, storing and using personal data in the first place.

67 Additionally, the cost of disclosing personal data may be shared between the company and the data recipients in various ways. A recipient may be required to pay a specified sum to cover a company's costs in processing data (*eg*, to anonymise data where possible). Each data recipient may also be required to give a standard list of undertakings, which helps reduce a company's cost of negotiating with each recipient to protect its commercial interest. This list should include, for instance, an undertaking not to disclose data to any other person without prior consent from the company.[137] While many of the understandings would resemble terms contained in a commercial data sharing agreement, the key difference is that the company no longer has the final say in deciding whether to share data in these limited circumstances.

(2) To reduce anti-competitive conduct

68 More controversially, it has been suggested that companies should sometimes be required to grant outsiders access to the data in its possession to promote competition. One important question is whether the mere possession of a database can have anti-competitive effects. Some believe that it can, pointing out that a company might be the only party capable of collecting the type of data in its possession and that consumers might be reluctant to switch to another database due to network effects.[138] Others argue that there are often alternative ways to collect the same data; for example, in addition to Google and Facebook, mobile service providers also have good access to their users' location data.[139] Moreover, the data collected by two companies might appear unique for one purpose, but fungible for another. Again, take Facebook and Google as an example. Google and Facebook offer different services and the types of data they generate through those services are different; however, from an advertiser's perspective, both companies offer essentially the same product, that is, more accurate identification of potential customers, and therefore substitutable.[140]

---

137 A detailed discussion of the scope of such a common property right is outside the scope of this article.

138 Daryl Lim, "Re-Defining the Rights and Responsibilities of Database Owners under Competition Law" (2006) 18 SAcLJ 418 at 422–444, paras 6–7.

139 Geoffrey A Manne *et al*, "ICLE Comments, FTC's Hearings on Competition and Consumer Protection in the 21st Century" *Social Science Research Network* (2019) at p 7 <https://papers.ssrn.com/abstract=3384794> (accessed 4 August 2020).

140 Geoffrey A Manne *et al*, "ICLE Comments, FTC's Hearings on Competition and Consumer Protection in the 21st Century" *Social Science Research Network* (2019) at p 9 <https://papers.ssrn.com/abstract=3384794> (accessed 4 August 2020).

69 Even where the possession of a database has anti-competitive effects, forcing a company to grant others access to its database (*eg*, through a compulsory licensing regime) may not be the only, or the most appropriate, remedy. The benefit of improved access to data must be weighed against other key considerations, including the likelihood that forced data sharing would have a chilling effect on innovation, increase the risk of cartelisation, or undermine the privacy interests of the relevant data subjects.

70 In light of the above considerations, whether a company should be required to share the data in its possession to curb anti-competitive conduct often has to be decided on a case-by-case basis. It has been suggested that a company should only be required to do so in limited circumstances, for example, where the database in question amounts to an "essential facility" and where a company's refusal to grant access to that database is likely to cause substantial harm to competition.[141]

VI. Conclusion

71 This article makes a case for examining personal data from a property law perspective. While property law is not a panacea for all the problems that have arisen in the big data era, it provides a useful framework and a set of established principles for approaching those problems. Nevertheless, further research is required to clarify the scope of an individual's private property rights in the data about him, as well as the conditions under which common property rights should be granted over personal data held by a company.

---

141 Law Reform Committee, Singapore Academy of Law, *Rethinking Database Rights and Data Ownership in an AI World* (July 2020) at paras 2.51–2.54.