Singapore Journal of Legal Studies
[2020] 90–114

THE BASICS OF PRIVATE AND PUBLIC DATA TRUSTS

JEREMIAH **LAU**, JAMES **PENNER** and BENJAMIN **WONG***

The term "data trust" has recently come into circulation to denote some kind of legal governance structure for the management of data, in particular digital databases, but there is much uncertainty and confusion about what a data trust is supposed to be, legally speaking. This paper examines the nature of data as a possible trust asset, and concludes that the traditional trust, the historical creation of English Equity jurisprudence and now found around the world, is a perfectly sensible vehicle for the management of data, in particular the management of combined datasets for both private and charitable purposes, especially educational purposes. The paper also considers the data protection issues that arise in relation to data trusts.

I. INTRODUCTION

And what rough beast, its hour come round at last, slouches towards Bethlehem to be born?[1] Why, the data trust of course. And it is a very rough beast indeed. We hope to shed some light on its nature in this paper. But we will begin with some reasons why people have started to care.

The term "data trust" first appeared around 2016.[2] This must primarily be attributed to the recent fascination with data, as opposed to any renewed interest in trusts. The importance of data to the modern economy is well documented and needs not be rehashed here. In fact, it would be silly to say that data or information is only *now* crucial to business. It always has been—Nathan Rothschild's early knowledge of the British victory at Waterloo and the killing he subsequently made buying government bonds illustrate this nicely.[3] The question is one of scale and scope.

---

* Jeremiah Lau and Benjamin Wong are Sheridan Fellows at the Faculty of Law, National University of Singapore. James Penner is Kwa Geok Choo Professor of Property Law at the Faculty of Law, National University of Singapore. The authors gratefully acknowledge the financial support of the National University of Singapore Faculty of Law-University of Toronto Faculty of Law Research Partnership.

1 W B Yeats, *The Second Coming*.

2 See Neil Lawrence, *Data Trusts*, online: Inverse Probability <http://inverseprobability.com/2016/05/29/data-trusts#fn:origin>. According to the blog post, "the idea of 'data trusts' emerged in conversations on data ethics between the blog author and Jonathan Price, barrister at Doughty Street Chambers in February and March 2015."

3 The story goes (and elements of this have become apocryphal in the re-telling) that Nathan Rothschild received news of the British victory over Napoleon's forces at the Battle of Waterloo by private carrier pigeon (or his own horsemen), in advance of the official government communique. He then sold the government bonds he held, causing a panic and inducing others to sell and hence a fall in the price, before buying them all again for a song. The news of the British victory finally reached the London Stock Exchange, and the price of the bonds soared, making Rothschild very rich indeed.

The kinds of data that we consider useful today would be unimaginable to someone from the past (try explaining to Nathan Rothschild how someone's 'internet cookies' might be commercially valuable data), and we have the means to extract, process, store, and analyse data on a truly industrial scale.

Suffice to say, to be "data-driven" is now a term of high praise. It shows up in national campaigns, company mission statements and LinkedIn profiles.

In 2017, the United Kingdom ("UK") Government commissioned a report entitled "Growing the Artificial Intelligence Industry in the UK".[4] This report recommended the use of data trusts to facilitate the sharing of data between organisations who hold data and organisations who are in a position to exploit that data in the development of Artificial Intelligence. There are two things to note about this report. First, it seems to have driven a lot of the subsequent interest in data trusts. Second, it offers a somewhat coy definition of "data trusts": "a set of relationships underpinned by a repeatable framework, compliant with parties' obligations, to share data in a fair, safe and equitable way".[5]

The report also outlines the role of a 'trustee', someone who helps manage the data trust, and emphasizes that the data trust is "not a legal entity or institution".[6] Equitable, has a trustee, composed of a set of relationships, not a legal entity? That sounds awfully similar to the trust as understood by the Chancery jurisdiction. But the report stops short of expressly saying so, and it is unclear if the report really does mean a trust that an equity lawyer would recognise (hereinafter referred to as "equity's trust"). We will return to this point later.

After the 2017 report came two other reports of note. The first was produced by Sidewalk Labs in 2018, entitled "Digital Governance Proposals for Digital Strategy Advisory Panel ("DSAP") Consultation" (hereafter referred to as the "Sidewalk Labs Proposal" ("SLP")).[7] The second was commissioned by the Open Data Institute ("ODI") in 2019, entitled "Data trusts: legal and governance considerations" (hereafter referred to as the "ODI Report").[8]

These two reports are representative of two distinct directions that the "data trusts project" seems to be headed in.

First, there is the Sidewalk Labs Proposal. Sidewalk Labs is a subsidiary of Alphabet Inc (which is itself the parent company of Google and several former Google subsidiaries). Sidewalk Labs is involved in developing Quayside, a site in Toronto's East Bayfront neighbourhood. Quayside is intended to be a "smart city".

Concerns were raised. Some of these concerns centered on the perceived asymmetry in power between Google and the city of Toronto[9]—the big tech company

---

4 See Wendy Hall & Jérôme Pesenti, *Growing the artificial intelligence industry in the UK*, online: Government of the United Kingdom <https://www.gov.uk/government/publications/growing-the-artificial-intelligence-industry-in-the-uk>.

5 *Ibid* at 46.

6 *Ibid*.

7 Sidewalk Labs, *Digital Governance Proposals for DSAP Consultation*, online: Sidewalk Labs <https://waterfrontoronto.ca/nbe/wcm/connect/waterfront/41979265-8044-442a-9351-e28ef6c76d70/18.10.15_SWT_Draft+Proposals+Regarding+Data+Use+and+Governance.pdf?MOD=AJPERES>.

8 BPE Solicitors, Pinsent Masons & Chris Reed, *Data trusts: legal and governance considerations* (2019), online: ODI <https://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf>.

9 David Rider, "The risks of becoming a Google city" *The Star* (5 March 2018), online: The Star <https://www.thestar.com/news/gta/2018/03/02/the-risks-of-becoming-a-google-city.html>.

extracting value from the city, and the city not getting much in return. Other concerns were directed at the sensors and cameras which would be installed in the smart city—these raised red flags about data protection and privacy more generally.[10]

The SLP began by highlighting several concerns and questions that surfaced with regard to data and the Quayside project. Amongst these concerns were the following:

> Is Sidewalk Labs and this project intended to be a data source for Google? How will data—particularly data collected in the physical environment, which some argue should be considered a public asset—be protected and governed? Who will own and control the data that originates in Quayside's physical environment? How do we address the difficulty of obtaining consent when collecting data in the physical environment? How do we make sure the protections of Canadian law apply to all data originating in Quayside?[11]

The SLP then sets out a framework for digital governance in Quayside, which includes four key components—(1) Responsible Data Use Guidelines; (2) Civic Data Trust; (3) Responsible Data Impact Assessment; and (4) Open Standards.[12]

The Civic Data Trust is defined in the SLP as a "model for stewardship and management of data and digital infrastructure that approves and controls the collection and use of data for the benefit of society and individuals".[13] It is "particularly useful where data is being collected and used in an urban environment and there are challenges in obtaining meaningful consent."[14] It is an "independent third party that ensures that value from data goes to the people, communities, government, industry and society from which it was collected, and that data privacy and security are protected."[15]

So it is reasonably clear that the Civic Data Trust, as envisioned by the SLP, is part of a larger strategy meant to address the concerns raised about data collection in the Quayside project. It particularly addresses (a) the challenge of obtaining meaningful consent and (b) the question of who benefits from the data collected.

Second, there is the ODI Report. The ODI Report sees that the "primary purpose of a data trust is to solve one of the fundamental problems faced when utilising machine learning".[16] This fundamental problem is the problem of data sharing. Many useful data sets are held in silos, some public and some private. As the report says, "Machine learning which uses these data sets, whether individually or as a combined dataset, is likely to generate insights which could not be achieved if each organisation were restricted to using only its own data."[17]

Therefore, the main purpose of the data trust, as envisioned by the ODI Report, is to overcome the challenges that impede the sharing of data. These challenges involve:

---

10 Editorial, "The Guardian view on Google and Toronto: smart city, dumb deal" *The Guardian* (5 February 2018), online: The Guardian <https://www.theguardian.com/commentisfree/2018/feb/05/the-guardian-view-on-google-and-toronto-smart-city-dumb-deal>.

11 *Supra* note 7 at 7.

12 *Ibid* at 10.

13 *Ibid* at 12.

14 *Ibid.*

15 *Ibid*.

16 *Supra* note 8 at 10.

17 *Ibid.*

respecting the intellectual property rights of owners of data sets, and incentivising them to share access to their data sets; protecting the rights that accrue to individuals in relation to their personal data; and protecting the confidentiality of information.

Would it be fair to say that the ODI Report foresees a far more 'commercial' use of the data trust than the Sidewalks Labs Proposal? Perhaps. It may be more accurate to say that the SLP foresees a more preventative use of data trusts, whereas the ODI Report focuses on a more facilitative purpose.

It will be apparent from the foregoing that the term 'data trust' is currently used for various purposes in literature. This implies that there are different conceptions of what legal form a 'data trust' should take. One attempt to bring some clarity to the concept has been to say that what is meant by a 'data trust' is *not* the trust as recognised by equity, and *cannot be*, because there are certain legal difficulties with employing equity's trust to achieve the ends that data trusts are meant to achieve. Settlors, beneficiaries, trustees, equitable—these terms of art are used in a metaphorical sense only. In the next part we will demonstrate why the concerns about employing equity's trust are misguided.

II. The Perceived Legal Difficulties with Equity's Trust

In the ODI Report, the claim was made that "trust law is not an appropriate legal structure for data trusts".[18]

Two reasons were given. The first is as follows:

> [F]irst, a legal trust must be run for the benefit of the beneficiaries, not the wider public. The exception to this is a charitable trust, which we have not examined because the restrictions of charity law mean that a charitable trust would only be suitable for a minority of data trusts. For an ordinary legal trust, trustees are required only to consider the collective interests of the beneficiaries when dealing with trust property. This means that they cannot allow data to be used for some socially beneficial purposes if that use does not also benefit the legal trust's beneficiaries, i.e. those described in the trust deed.[19]

The "restrictions of charity law" are referred to without further explanation, and so we can only guess at what reservations the authors had in mind. We will assume that the concern was with the rule that property settled on a charitable trust must only be used for charitable purposes. This would exclude 'private' purposes, and would also preclude the trust from having any individually entitled beneficiaries who could enforce the trust. Of course, many persons often *factually* benefit from charitable trusts, such as those who receive benefits under a trust for the relief of poverty, or students who benefit from educational trusts. Nevertheless, such individuals are not *legal* beneficiaries of the trust, and do not have standing to enforce the trust. The Attorney-General (or his delegate, such as a Charity Commission) enforces charitable trusts on behalf of the public.[20]

---

18 *Supra* note 8 at 8.

19 *Ibid* at 12.

20 See James Penner, *The Law of Trusts,* 11th ed (UK: Oxford University Press, 2019) at para 14.3 [Penner, *Law of Trusts*].

Accordingly, the mere fact that property is settled on a charitable trust does not preclude the settlor from factually benefiting from the use of that property. It simply means that the settlor no longer has a beneficial interest in the property, or to put it another way, the settlor no longer has the right that the property should be used for his own private benefit.

Another sense in which the law of charities might be 'restrictive' is that the purpose for which the property is to be used must be 'charitable'. It is true that there are well-developed legal requirements that govern what the law considers charitable. These are traditionally known as the four 'heads' of charity—the relief of poverty, education, religion, and other purposes beneficial to the public.[21] However, the law of charities is more expansive than some realise. There is good news for those interested in using data trusts to facilitate the sharing of data for research. Carrying out useful research is a charitable purpose under the head of 'education'.

The second reason given by the ODI report against the usefulness of equity's trust is as follows:

> [S]econd, the trustees are obliged not to use the property of the legal trust in a way which generates benefits for themselves unless the trust deed specifies otherwise. This means that providers and users of data will find it difficult to be trustees if they are envisaging benefits for themselves as a result of data sharing. This is likely to deter many organisations, particularly data providers, from participating. The requirement that (subject to the trust deed) any financial benefit received as trustee may not be retained but becomes trust property, is an obvious reason why this form of data trust is unlikely to be viable for commercial actors.[22]

This objection is far easier to deal with, because it is clearly wrongly conceived.

It is trite law that a trustee can also be a beneficiary under a trust. A settlor can settle property to be held on trust by trustee T, for the benefit of beneficiary B and trustee T (who, in this capacity, is as much a beneficiary as beneficiary B). What is *not* possible, is for trustee T to hold trust property on trust for herself only—she cannot be the sole trustee and the sole beneficiary.[23]

What the ODI report *may* be concerned with is the rule that trustees, as fiduciaries, may not profit from their trust.[24] This rule does not mean that trustees cannot be properly remunerated, otherwise professional trustees would not exist. It does mean that trustees (or fiduciaries more generally) cannot make unauthorised or secret profits from their position.[25] Examples from the case law include the taking of bribes[26] and

---

21 This will be elaborated upon in more detail in 3.2, below.

22 *Supra* note 8 at 12.

23 Penner, *Law of Trusts*, *supra* note 20 at para 2.3.

24 On the law governing fiduciaries and its application to trustees see Penner, *Law of Trusts*, *supra* note 20 at paras 2.19-2.26 and ch 13. See also James Penner, "Distinguishing Fiduciary, Trust and Accounting Relationships" (2014) 8 Journal of Equity 202.

25 A related rule, the "no conflict" rule, would also prevent trustees, as fiduciaries, from acting in situations of potential or actual conflict of interest. These situations can (usually) be avoided by obtaining the beneficiary's consent after a process of full disclosure.

26 *The Attorney General for Hong Kong v Charles Warwick Reid (New Zealand)* [1993] UKPC 2.

the usurping of corporate opportunities.[27] It is not clear how these rules would deter the sharing of data by commercial organisations.

III. The Nature Of Data And How Data Can Be A Trust Asset

A. *Information and Data*

Just by being the observant and social creatures that we are, we have endless amounts of information about other identifiable living individuals, even if we have not recorded that information anywhere, by writing it down, for instance, or storing it in a computer file. And as relational beings, we use this information on a regular basis—for example, when we have a conversation in which an individual is a topic of discussion. The basic point is that we possess information about a great many things, people included, from many sources,[28] and apply this information in our daily lives in countless ways. Evidently, it would be meaningless or totalitarian for the law to attempt to regulate completely our use of personal information.

There are, nonetheless, laws that constrain our use of personal information. Chief among these is data protection law, a legal innovation that has expanded and proliferated over the past few decades. At the present time, the majority of developed economies around the world have enacted data protection legislation of some sort. Data protection laws have a very broad remit—for example, the European Union's ("EU") General Data Protection Regulation ("GDPR") professes to regulate the processing of personal data.[29] "Processing" under the GDPR means any "operation or set of operations" performed on information, and this is sufficiently broad to include anything that could be done to personal data.[30] "Processing" includes, but is not limited to: "collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".[31] Canadian data protection legislation regulates the "collection, use and disclosure" of personal data, which is arguably narrower than "processing",[32] but it is unlikely that the difference is significant in practice. "Personal data" is similarly given a broad definition under the GDPR as "any information relating to an identified or identifiable natural person".[33] It includes both objective and subjective information about a person, may be true or false, and encompasses information in

---

27 *Bhullar v Bhullar* [2003] EWCA Civ 424.

28 For an excellent discussion of knowledge, information, belief and memory and their interrelationships see Hacker PMS, *The Intellectual Powers: A Study of Human Nature* (UK: Wiley Blackwell, 2013) at ch 4-6 and 9.

29 *General Data Protection Regulation,* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, art 1(1) [*GDPR*]. The UK *Data Protection Act 2018*, c 12 implements and supplements the GDPR in the UK.

30 *Ibid*, art 4(2). See Rosemary Jay, *Data Protection Law and Practice* (UK: Sweet & Maxwell, 2012) at 178. It should be noted that processing "by a natural person in the course of a purely personal or household activity" is excluded (see *GDPR*, *ibid*, art 2(2)(c)).

31 *GDPR*, *supra* note 29, art 4(2).

32 *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, s 3 [*PIPEDA*].

33 *GDPR*, *supra* note 29, art 4(1). There are particular definitional problems as to what it means to say that information "relates" to a natural person, and as to when a natural person is "identified or identifiable" from information, but these problems are beyond the scope of this paper.

all formats.[34] Canadian data protection legislation again adopts a slightly narrower definition—under the Personal Information Protection and Electronic Documents Act ("PIPEDA"), personal information means "information about an identifiable individual".[35]

While it would appear, at first glance, that the GDPR exerts total control over the use of personal data, there are important substantial limits that have been built into the GDPR. In terms of material scope, the GDPR does not apply to processing by natural persons in the course of a purely personal or household activity,[36] and it only applies to processing that is at least partly automated or where the personal data processed forms part of a filing system.[37] The rules of the GDPR are, furthermore, subject to the fundamental rights.[38] Despite these limits, however, it remains the case that the GDPR has a very large footprint, and imposes a significant constraint on activities involving personal data. The same may be said of the data protection laws of other jurisdictions.

Data protection law aside, the other legal rules governing our use of personal information are located across the various fields of law. Tortious liability is imposed for the misuse of private information and for defamation; criminal law inflicts sanctions on persons who disclose certain sensitive information contrary to official secrets legislation; contractual and equitable obligations of confidence bind parties in a wide variety of circumstances, ranging from employment relationships to business negotiations.

One field of law that has not, however, historically been engaged in the regulation of the use of personal information (or, indeed, information generally) is the field of property law. This is because information has not been regarded as a kind of property.[39] In making this point in the context of treating information as a trust asset, Lord Upjohn had this to say:

> I shall refer to the judgment of Russell L.J. . . . He said:
>
> "The substantial trust shareholding was an asset of which one aspect was its potential use as a means of acquiring knowledge of the company's affairs, or of negotiating allocations of the company's assets, or of inducing other shareholders to part with their shares. That aspect was part of the trust assets."

---

[34] Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data,* Working Paper WP 136 (2007) at 6-7, online: GPDP <https://www.gpdp.gov.mo/uploadfile/others/wp136_en.pdf>. The format of the personal data has an indirect relevance in that the GDPR only applies to the "processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system" (see *GDPR*, *supra* note 29, art 2(1)).

[35] *PIPEDA,* s 2(1). See also *Personal Information Protection Act*, SA 2003, c 65 [*ABPIPA*] and *Personal Information Protection Act*, SBC 2003, c 63 [*BCPIPA*].

[36] *GDPR*, *supra* note 29, art 2(2)(c).

[37] *GDPR*, *ibid*, art 2(1).

[38] *GDPR*, *ibid*, recital 4.

[39] For a discussion of this in relation to cryptoassets, see UK Jurisdiction Taskforce, *Legal Statement on cryptoassets and smart contracts* (2019), online: The LawTech Delivery Panel <https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf>.

> My Lords, I regard that proposition as untenable.
>
> In general, information is not property at all. It is normally open to all who have eyes to read and ears to hear. The true test is to determine in what circumstances the information has been acquired. If it has been acquired in such circumstances that it would be a breach of confidence to disclose it to another then courts of equity will restrain the recipient from communicating it to another. In such cases such confidential information is often and for many years has been described as the property of the donor, the books of authority are full of such references; knowledge of secret processes, "know-how," confidential information as to the prospects of a company or of someone's intention or the expected results of some horse race based on stable or other confidential information. But in the end the real truth is that it is not property in any normal sense but equity will restrain its transmission to another if in breach of some confidential relationship.[40]

A duty of confidence arises only between specific individuals, and so no duty is generally breached by a third party to whom the information is revealed in breach of that duty.[41] That is to say, the confider of the information has no claim against third parties who acquire the information after it has been wrongfully revealed—she cannot say to those parties, "This information is mine, and you cannot use it". The law could also be said to 'regulate information' in the intellectual property realm, as for example in the case of patents. Someone who is not a holder of a patent or a licensee of the patent holder is prohibited from making use of the information disclosed in the patent to work the invention. But of course, it being a *patent*, *ie,* a disclosure of the invention, means that anyone can read the information it discloses and use that information for any purpose other than working the invention.

Be all that as it may, we can restrict our attention to information that is recorded, specifically information that is recorded in digital files. In an excellent paper,[42] Michels and Millard ("M&M") explain the way that private law protects information so recorded.

M&M distinguish first between three levels at which a digital file exists.[43] At what they call the 'hardware layer', a digital file "has a persistent existence on a physical storage medium",[44] in terms of a series of ones and zeroes which can be decoded by access software to reproduce the text you see on your computer screen, or what you hear (in the case of audio files) or see and hear (in the case of video files) when you hit 'play'.[45] The storage media are various, from a USB key to the hard drive on your computer to servers at a distance, accessed through the internet or via your mobile phone company's network. It is important to note that, regarding servers at

---

40 *Boardman v Phipps* [1967] 2 AC 46 at 127-128 (HL) [footnotes omitted]. See also *Oxford v Moss* (1979) 68 Cr App Rep 183 at 185-186; *Your Response Ltd v Datateam Business Media Ltd* [2014] EWCA Civ 281 at para 42; *OBG Ltd v Allan* [2007] UKHL 21 at para 275.

41 A third party may be liable in such a case for the tort of inducing a breach of contract, for example.

42 Michels JD and Millard C, "Mind the Gap: The Status of Digital Files Under Property Law" (2019) Queen Mary University of London, School of Law Legal Studies Research Paper No 317/2019 [*M&M*].

43 *Ibid* at 5-7.

44 *Ibid* at 6.

45 *Ibid*.

a distance, the digital file may be fragmented across different servers[46] (fragments which the access software can re-integrate), and a file might be copied to multiple servers either for back-up or to make a retrieval of the file via the access software speedier.[47]

M&M next define a "virtual" layer, which basically integrates the physical recording of the digital file with the operational software which brings the recorded file to the user:

> At the virtual layer, a desktop G[raphical] U[ser] I[nterface] invites users to imagine that the screen is an actual desktop on which they carry out actions analogous to those occurring on a physical desktop, such as opening and closing folders or disposing of unwanted material into a wastebasket.[48]

This is the level at which a digital file user can access and manipulate the content of the digital file.

Finally, there is the 'content' layer. This is essentially the information which the digital file presently records. This is the content that could, for example, be copied, printed out, and so on and is defined by the information it contains. Importantly, as the example of printing a text or picture file shows, unlike the digital file at the hardware or virtual layers, the content of a file 'floats free' from any particular mode of recording it. Any mode of recording will do so long as it preserves the informational content.[49] For example, a picture file can be stored as a pdf or jpg, and these different files will be recorded at the hardware level in terms of different ones and zeroes so as to be compatible with the access and manipulation software pertaining to each.

M&M acknowledge that information per se is not a kind of property for the reasons canvassed above, but then ask whether the law protects what might be called 'privileged access' to information recorded in digital files. They rightly point out several things. First, in the same way that my privileged access to the personal information I record in my diary is protected by my ownership of the diary itself, my privileged access to the ones and zeroes stored on USB keys, hard drives, and servers, is similarly protected by the property rights in those physical things. This brings us to the question of use rights in our tangible property.

A person who owns tangible property like land or goods is at liberty to use her property subject to general regulations on the use of things. A person may not use a knife to wound another or drive a car above the speed limit. This has nothing to do with ownership or property rights. A thief of a knife or car just as much as their owners is prohibited from doing either of those things. But the flipside of this point is that so long as a person stays within the law, she may do anything she wants with the tangible property she owns. In particular, a person who owns land or a chattel does

---

46 *M&M*, *supra* note 42 at 10.

47 *Ibid* at 25.

48 *Ibid* at 6-7.

49 Although, of course, different recording modes will have different strengths and weaknesses. Books do not crash, but they wear out with use. MP3 files do not deteriorate with use, but some people still prefer vinyl. And so on. The upshot is that some information may be lost in moving from one recording format to another.

not have a legally recognised list of 'use rights' to which she is entitled and which she can legally enforce. Within the kind of general prohibitions just mentioned, the liberty to use the tangible property you own is unregulated by law.[50] What her title to her property consists in or of is a right that others not interfere with her property, plus two powers of title: the power to license others to do what would otherwise be a trespass—to invite friends over to dinner, to lend a friend a jacket—and the power to transfer her title to the property to someone else.[51] Here we are concerned with the protection afforded by the right that others not interfere with the property she owns. It *does* protect her liberty to use her property in any way she chooses, within the limits the law places on prohibited uses of things, but it does not make any individual use she wishes to make of her property into a legally recognised use right.[52] The right that others not interfere with the property one owns is complex, and framed in the law of wrongs, the law of torts. Interference is framed in three sorts of ways—I wrong you if I use your property as my own, in a sense 'usurping' your property, or by damaging your property either intentionally or negligently, or by depriving you of your property rights, say by detaining it so you are unable to get access to it.[53] Obviously, all of these torts, these wrongs, apply to the physical devices upon which data is recorded, from servers to USB keys. But notice that this private law protection does nothing to *ensure* that your access to your data remains intact. If you forget your password, or the USB key becomes corrupted, the law does nothing to help you. Your liberty or ability to use your data is not supported by the law in that sense. It only protects your use indirectly by prohibiting the incursions of others on the physical things in which your data is recorded, just as is with the case of the hand-written entries in the physical book that is your diary.

Private law also protects a person's right to the content layer, in one specific and in one general way. Specifically, one may enter into a relationship of confidence with another party such that the confidee of information undertakes an obligation not to disclose that information to third parties. We have already discussed this relationship above. More generally, copyright subsists in any original work, and work is broadly defined to include useful formatting, organisation, or presentation of general information,[54] and databases.[55] Copyright protects the creator of an original work by prohibiting others from making copies of the work or communicating it to the public.[56] It is important to note that these are genuinely protections of the content layer. It does not matter the form in which one breaches confidence or copyright. A photograph of a painting or hand produced copy are equally prohibited, and one breaches a confidence equally if the confidential information is transmitted orally or in writing.

Now what about the virtual layer? As we have already seen, the virtual layer is the layer at which one *uses* the digital file, to play it or manipulate it. The virtual layer

---

50 James Penner, *Property Rights: A Re-Examination* (New York: Oxford University Press, 2020) [Penner, *PRAR*] at para 3.2.

51 Penner, *PRAR*, *ibid* at para 1.2, 1.4.

52 Penner, *PRAR*, *ibid*, ch 1 and ch 7.

53 Penner, *PRAR*, *ibid*, ch 7.

54 *Copyright, Designs, and Patents Act 1988* (UK), c 48, s 3(1)(a).

55 *Ibid* at ss 3(1)(d), 3A.

56 *Ibid* at ss 16(1)-(2).

therefore reflects the *use rights* that an individual with access to the digital file has. And just as with property in chattels or land generally, the law neither enumerates nor protects unregulated use rights of this kind. The only exception to this is criminal law provisions making hacking an offence. These do prevent another gaining authorised access to digital files, thereby prohibiting unauthorised copying, manipulation, or destruction of digital files,[57] and so in that sense can be seen to protect an individual's authorised use of digital files.

B. *The Licencing of Access to and "Transfer" of Digital Files*

Let's return to our example of a diary. Ben can license what would otherwise be an unlawful interference with his diary. Ben can license you to handle, open, and copy the information in it. Ben could also just give or sell you the diary, transferring his title in it to you. Ben would still retain copyright in the writing, but Ben could transfer that copyright to you as well.

When Ben transfers title to you, you acquire the power of title to transfer the diary yourself in turn. The power to transfer goes with having title. By contract Ben and you can agree that you will not transfer the property, but you still have the legal power to do so. If you transfer the diary to a third party you commit a breach of contract, but the transfer is still effective.

The case of licences is different. A licence can either be transferrable, or to use a term meaning the same thing, 'assignable', or not. Consider theatre tickets. A theatre ticket is just a contractual licence to enter the theatre and attend the performance, usually requiring you as a term of the licence to occupy a particular seat. These licences are typically not assignable as a matter of the terms of the contractual licence. Only the person to whom the ticket is sold has the right to the licence, to attend the performance. But people do give away or sell their theatre tickets to others who do attend the performance. Strictly speaking, in law, these holders of the tickets are not entitled to attend, for the licence was not assignable. But theatres typically do not press their legal rights, and do not bother about who attends as long as they have a valid ticket for the performance.

The same is true with Ben's licensing you to read his diary. Typically this will not be an assignable licence. Ben lends the diary to you for your own purposes, not to anyone else. Any other person to whom you passed the book would be liable for interfering with Ben's chattel. Software licences, the licence to use Microsoft Office for example, are also typically not assignable. So even though it is perfectly possible to confer upon another an assignable licence to your property, for a host of obvious reasons this tends to be atypical.

Now consider this in relation to digital files. The closest analogy to the diary case is a possible dealing with a USB key. Ben can transfer the key itself to you, and you thereby acquired a physical device with the zeroes and ones recorded as Ben created them. But Ben does not transfer the means of creating the virtual and content layers of the digital files therein encoded. You have that yourself and use your own access and manipulation software when you plug the data key into your computer. In the same way when Ben gives you his diary, Ben does not give you the means to read

---

[57] *Computer Misuse Act 1990* (UK), c 18, s 1.

it. You do that with your own eyes and mind. Similarly, Ben can license you to use the USB key, perhaps to make copies of his digital files.

Perhaps, most typically, we 'transfer' digital files by sending them to someone, by email over the internet, for example. As M&M explain, however, this is not any kind of property transfer.

> Alice can . . . use a file transfer protocol to deliver the file to Bob. In that case, the file is not physically sent to Bob. Instead, Alice's computer will send the instructions required to create a copy of the file on Bob's computer. To do so, Alice's computer will send a string of packets containing ones and zeros to Bob's computer, typically via a series of internet routers. The ones and zeros are expressed by modulating a signal, such as an electrical charge across a copper wire, a beam of light across a fibre optic cable, or electromagnetic waves in the case of wireless networks. Bob's computer receives the instructions and reassembles the file by storing ones and zeros on its hardware in the right order. In doing so, a second file with identical content is created on Bob's computer, with a new file name and access path. Thus, the result of a virtual transfer is the creation of a second file on the recipient's device. Alice will retain her original file (unless she deletes it). The principle is similar to two people communicating in Morse code through a telegraph: binary signals are exchanged that represent a message, without any physical letter being sent.[58]

Not only is sending a digital file this way not a transfer of any kind, it is not analogous to a licence either. What Alice does in this case is to *do something* which results in Bob's being able to make his own copy of the digital file. One analogy would be Alice's turning up to a public park so that Bob can take a photo of her. Whilst as a matter of politeness Bob should ask Alice if he can take her picture, in law Bob requires no permission or licence from Alice in doing so. He is at liberty to take any picture he wants so long as in doing so he does not breach some other law, such as the law against trespass. So what Alice does is just give Bob an opportunity by showing up—he can then record her image for himself.

Perhaps a closer analogy is the following. Assume Alice and Bob are workmates who have access to a company scanner, and Alice wants to 'send' a copy of a document to Bob. The document never leaves her possession. She puts it on the scanner flatbed, closes the cover and then lets Bob enter his email details and hit 'Scan'. After the scan, she retrieves the document. Again, Alice does something so that Bob can use the connectivity of the scanner to acquire a copy for himself, but she transfers nothing and does not license Bob to so much as touch anything of hers. (Of course if she hands the document to Bob to do this all himself, she does license him to do what would otherwise be an interference with her chattel, the document.)

This way of seeing things is reflected in two fairly recent English judgments.

In *Fairstar Heavy Transport NV v Adkins*,[59] the managing director of a company used his own personal email account to send emails relating to the business. After the termination of his appointment, the company sought access to the business emails and

---

[58] *M&M*, *supra* note 42 at 10.

[59] [2013] EWCA Civ 886.

succeeded. The case was decided upon contractual, specifically, agency principles, with the court holding that in virtue of the agency relationship the former managing director was required to provide access to the emails relating to the business.

In *Your Response Ltd v Datateam Business Media Ltd*,[60] the defendant demanded access to digital files held by the claimant, a data management company. The claimant was owed money under their contract and claimed that it had a 'lien' over the files until it received payment. A lien is a kind of possessory self-help remedy. For example, the repairer of a vehicle is entitled to a lien, the right to retain possession of the vehicle, until paid for his repairs.[61] The Court of Appeal held that since digital files were not tangible property of any kind, no such lien could exist.[62] More importantly for our present purposes, the Court held that such rights to access that the defendant held were a matter of the contract between the two parties, and that the claimant had committed a breach of contract in failing to provide access to the relevant files.

The point of the foregoing discussion has been to demonstrate that the various ways in which we have rights to access digital files can be the subject matter of interactions between different persons. Rights to access to digital files may be granted to others, in certain cases (as with the USB key transfer) by the actual transfer of property, but in other cases, surely most cases, not by a kind of licence, but by the creation of a contractual right that requires someone to 'make available' their digital files.

C. *Rights to Data as the Subject Matter of a Trust*

A basic principle of trusts law is that any right that has economic value can be a right held on trust. Easy cases of possible trust assets are property rights to tangible property, chattels and land, and intangible property such as debts, like the balance owing on one's bank account, company shares, and monopoly rights such as trademarks, patents, and copyrights. An easy case of a right that cannot be trust property is one's right to vote in Parliamentary elections, or your right[63] to choose whom to marry. In civilian systems like Quebec which also have a form of trust, the distinction is drawn between 'patrimonial' rights, which are rights which pertain to your 'economic personality', and 'extra-patrimonial' rights, such as your right to vote.[64] In common law systems, the distinction is less systematic, and is framed in terms of the question whether a right is 'personal' to the right holder. The question is sorted out in different contexts, but typically in the case of insolvency or death, where the question is whether a particular right of a person can be assumed by their trustee in bankruptcy if they become insolvent, or by their personal representative on their death. For example, a right to damages for wrongful dismissal is regarded as an economic right available to one's creditors in the case of one's insolvency, whereas the

---

60 [2014] EWCA Civ 281.

61 Bridge M, *Personal Property Law*, 4th ed (UK: Oxford University Press, 2015) at 270-271 [Bridge, *Personal Property Law*].

62 *Supra* note 60 at paras 9-34.

63 A 'power' in Hohfeldian terms.

64 Because a trust under the provisions of the Quebec Civil Code is a *patrimony* appropriated to a purpose, by definition it can only contain patrimonial rights. We thank Lionel Smith for his insight into the relevant provisions of the code, which we shall not discuss in detail here.

statutory right to be reinstated in one's job following an 'unfair dismissal' is personal to the employee.[65]

Nevertheless, the law of trusts tends to be fairly liberal about the kind of assets that can be held on trust. For example, a contract of personal service is not generally assignable. If you contract with me to give me a haircut next Tuesday, in general I cannot assign the right to that contractual performance to a third party. Nevertheless, in *Don King Productions Inc v Warren*,[66] the English Court of Appeal held that though unassignable, the obligee of such a contractual obligation could declare a trust over it.[67] Similarly, in *Barbados Trust Co Ltd v Bank of Zambia*,[68] the Court of Appeal held that a person, in this case a company, could declare a trust over an unassignable debt obligation.[69] As we shall see, in certain cases the assignability of rights to access data may arise to complicate the picture of how they might be available as trust assets.

How the benefits of a trust come to a beneficiary may vary, depending upon the trust assets that are held. Imagine that, under the terms of a trust, a trustee has a discretion to apply trust property to the benefit of one of the discretionary objects—call him Lionel. Suppose that the trustee thinks it would make sense for Lionel to have a new car. There are three ways in which this objective might be achieved. The trustee could just give Lionel money from the trust funds to buy a car for himself. Or the trustee could use trust funds to buy the car for Lionel, that is to pay the car seller on Lionel's behalf, so that Lionel acquires title to the car. Or the trustee could use trust funds to buy a car in the trustee's name, *ie* taking title to the car as a trust asset, and then licensing the car to Lionel to use. The last option would be the safest way of dealing with those irresponsible or feckless Lionels of this world whose existence or perceived existence preys upon the imaginations of fretful settlors—if Lionel had a bad gambling habit, for instance, keeping the car as trust property would prevent Lionel from selling it and blowing the proceeds playing online poker. Licensing the use of trust property also arises not infrequently in case of trusts of land. It may be a term of the trust that the trustee must or may exercise his power to licence the possession and use of the property to beneficiaries.[70]

---

65 *Grady v Prison Service* [2003] EWCA Civ 527.

66 [2000] Ch 291 [*Don King*].

67 The case is not particularly well reasoned, for two reasons. First, the court did not need to decide that the right to the contractual service *itself* was a trust asset—the court could simply have held that the economic benefit of the contract, *ie* the funds earned from the performance was the relevant trust asset, and this would have been a finding in accordance with trite property law and trust law principles. Second, a right to the personal service of a person is a kind of 'flawed' trust asset, since the only possible trustee is the obligee of the personal service. Or rather, the only possible 'custodian' trustee, the only trustee who could have title to the right in question would be that obligee. Any change of trustees in the case of the unfitness or death of the original trustee who declared the trust over the right in question could only be effected via the creation of a managing trustee/custodian trustee structure. See Penner, *Law of Trusts*, *supra* note 20 at paras 2.117 and 10.63.

68 [2007] EWCA Civ 148 [*Bank of Zambia*].

69 In *Bank of Zambia*, the point was also made at para 43 that a declaration of trust is not an equitable assignment.

70 Beneficiaries, simply in virtue of their status as beneficiaries, have no right to occupy or take possession of any of the assets of the trust. See James Penner, "The (True) Nature of a Beneficiary's Equitable Proprietary Interest Under a Trust" (2014) 27 Canadian Journal of Law & Jurisprudence 473 at 481-484; Penner, *Law of Trusts*, *supra* note 20 at paras 2.107-2.116.

In the case of digital files, licences and rights to access data can be trust assets. For example a person, called a 'settlor' of the trust assets, could transfer a USB key containing, let us say, text files concerning the family history, jpegs of family photos and so on, and the terms of the trust could empower the trustee, at his discretion, to provide possession of the key from time to time to beneficiaries. More plausibly than this licensing route to benefit the beneficiaries, the settlor could simply 'send' the digital files to the trustee imposing obligations on the trustee as to how they should continue to be stored and so on, with a term of the trust empowering the trustee to grant access to the digital files by sending them to the beneficiaries, imposing whatever conditions upon their access he thought fit.

A trickier case is the following. Take the case of Samantha, who has digital files stored on the cloud, that is with a remote data service company. Samantha declares that she holds her access rights to the files, again say containing files about the family, on trust for her children. It is almost certainly the case that Samantha cannot grant access rights to her children, third parties, under her contract with the cloud company. Revealing her password to others is also probably a breach of that contract, for example, and it is likely that she cannot assign her rights under the contract either. As we have seen with the cases of *Don King* and *Bank of Zambia*, this does not make the trust invalid, but it will give rise to complications.[71] Since the trusts we will be discussing in the next section will not be trusts of this kind, we shall not pursue this case further.

IV. Trusts Of Data

In this Part we will consider two sorts of circumstance in which someone might wish to set up a trust the main asset of which is the right to access digital files, in particular 'data sets', large numbers of files which accumulate certain kinds of data, for example the data sets gathered by entities such as social media companies, transportation providers like Transport for London or the Singapore Land Transport Authority, or mobile phone providers. We shall first look at private, 'joint venture' data trusts, and then at charitable data trusts.

A. *Private Joint Venture Data Trusts*

Let us assume that a company, Telco, has a data set, gathered from mobile phone users, which tracks their whereabouts, and another company, Transhub, has a data set with information about an urban transportation system, frequency of trains, usage patterns, and so on. They wish to pool their data sets and analyse the pool in order to create better algorithms for managing the trains, and perhaps to create apps which draw upon the combined data. They intend to share any profits received from the creation of the apps, and perhaps from increased revenue from the transportation system. What they can use to do this is a joint venture trust.

We can start with a more familiar model of such a trust, a joint venture trust to develop land. A, B, C and D enter into a joint venture to develop a plot of land,

---

[71] Bridge, *Personal Property Law*, *supra* note 61. See also *M&M*, *supra* note 42 at part 3.2.

Blackacre. In order to understand the trust structure they will use, we have to back up a little first to understand a particular kind of trust, the 'nomineeship'.[72]

First we must distinguish between 'bare trusts' and 'special trusts'. Under a bare trust, a trustee holds property for a beneficiary on no specific trust terms; the trustee's only obligation is to transfer the property to the beneficiary or to a third party as the beneficiary directs. In contrast, a special trust is one created by a settlor with specific terms; the standard example is the typical family trust, in which the trustee has various duties, to invest the trust property, to pay the income to X, and so on.

An intentionally created bare trust is called a 'nomineeship'. A nomineeship combines the bare trust with a contract. A nominee is a bare trustee who has contractually agreed to comply with various orders the beneficiary makes with respect to the trust property. Perhaps the most common example is the trust upon which a solicitor holds his client's purchase monies prior to completion of the sale of land. The solicitor holds the money in his client trust account, and the solicitor can only disburse the money according to his client's instructions under their contract (often called a 'retainer') and, in the case of a sale of land, this will be the instruction to transfer the money to the vendor in return for the transfer of title to the land. This is not a special trust.[73] But the solicitor here is more than a bare trustee: he has also undertaken by contract to deal with the property as the beneficiary directs. It is said that the nominee or bare trustee holds the trust property 'to the order' of the beneficiary and, while this is perfectly correct, it is important to notice that in the case of a simple bare trust the only order the beneficiary can make is an order to the trustee to transfer the property to himself or someone else, whereas in the case of the nomineeship the trustee has contractually undertaken to carry out different sorts of orders, which can be very extensive[74]; in such cases the trustee is also an agent of the beneficiary.

In order to structure the ownership of Blackacre and direct its development, A, B, C, and D will create a nomineeship.[75]

For ease of analysis, let us say that A, B, C and D (the owners) contribute equally to the purchase price of Blackacre, £1m each. Under the contract of sale of Blackacre, the vendor transfers title to the land to T, the trustee, a company incorporated for this particular joint venture. (Such one-purpose companies and trusts are often referred to as 'special purpose vehicles'.) T holds Blackacre on trust for the owners in equal shares, and the shares of T are also held in equal shares by the owners. Under the arrangement, T will act as agent for the owners in developing the land, entering into contracts with third parties, architects, builders and so on. There are different ways in which T, or rather T's directors, can be controlled so as to ensure the development of the land. One way would be for the owners to appoint a board of directors via voting on their shares, and allow these directors to exercise judgment on their behalf in developing the land. Or they could appoint directors, but give these directors instructions via a nominee committee, made up of persons appointed by the owners.

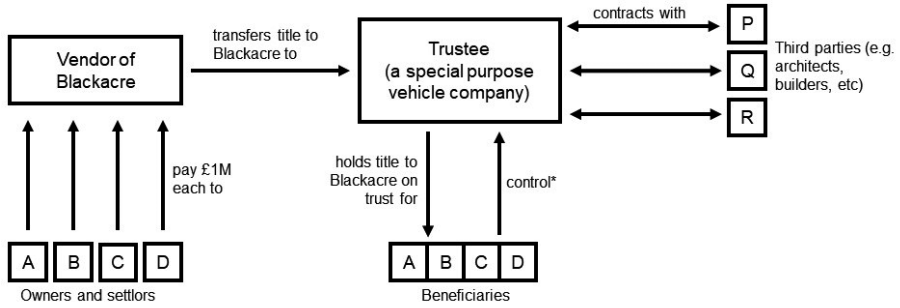
---

72 The following two paragraphs are modified from Penner, *Law of Trusts*, *supra* note 20 at paras 2.13-2.16.

73 See *AIB Group v Mark Redler & Co* [2014] UKSC 58 at 13.

74 See further Matthews P, "All about bare trusts: Parts 1 and 2" (2005) 6 Private Client Business 266.

75 For an example of a land development joint venture trust, see *Trident Holdings Ltd v Danand Investments Ltd* (1988) 49 DLR (4th) 1 (Ont CA); for a slightly more complicated trust structure for a joint venture between oil companies to own and run an oil refining and distribution facility, see *Shell UK v Total UK* [2010] EWCA Civ 180.



*by (i) voting onto the Trustee's board of directors individuals who are qualified and trusted to carry out the development of Blackacre, or (ii) forming a nominee committee which instructs the directors.

Fig. 1.

The owners will reap the benefit of this development in terms of the increase in the value of the land owing to its development, which will be realised by a subsequent sale to a third party or by leasing the developed land to third parties to create an income stream under the trust for the trust beneficiary-owners. See Figure 1.

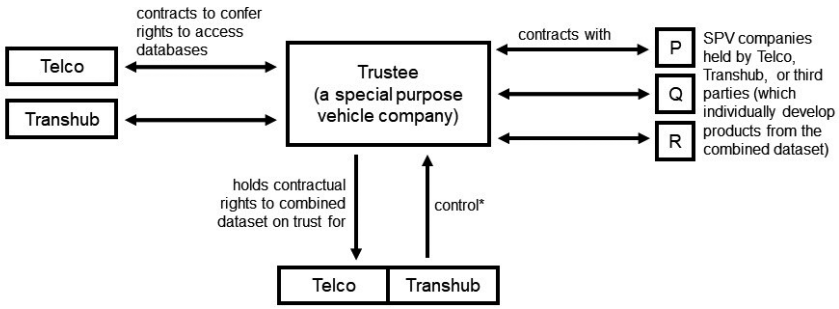
An essentially identical structure could be used to create a joint venture data trust. Telco and Transhub, the 'owners', will be the settlors of the trust. They could just 'send' discrete data sets in the form of masses of individual digital files to the trustee, but more plausibly, given that these data sets will be continuously updated, will enter into contracts[76] with the trustee giving the trustee rights to access their data sets on an ongoing basis. It is these access rights which are the trust assets. The trustee could hire third party individuals or companies to analyse the combined data sets to produce new algorithms or apps with the combined data, but more plausibly the trustee will take assignable contractual access rights and assign those rights to other special purpose vehicle companies, also owned by Telco and Transhub, to analyse the data in specific ways, to create one app or algorithm or another. The trustee could also contractually provide access rights to the data to independent third party companies on an upfront payment or profit-sharing basis. Granting such access rights to these special purpose vehicles would be on such terms and conditions as the trustee was instructed to impose by its directors or the nominee committee. In this way, Telco and Transhub can profit from the arrangement as owners of the special purpose vehicle companies which in turn own the developed apps and algorithms. See Figure 2.

B. *Public or Charitable Use of Data*

Similar structures can be used to create charitable data trusts. It is important to point out at the outset that charitable purposes can be carried out by trustees holding trust assets, or companies which hold assets. Both are equally bound by charities law to use their assets only for the charitable purpose for which those assets were transferred to the trustee or company.

---

[76] They could also enter into gratuitous but binding covenants granting the trustee access rights.



* by (i) voting onto the Trustee's board of directors individuals who are qualified and trusted to give access rights to third party-related SPVs for sound commercial purposes, or (ii) forming a nominee committee which instructs the directors.

Fig. 2.

Charities that take the form of trusts are exempt from several rules of trust law. Perhaps most significantly, they are exempt from what is known as the beneficiary principle, which states that every trust must have one or more legal persons as beneficiaries. Therefore, trusts which are set up not for any beneficiary but to pursue a purpose, are generally speaking invalid. Charities are exempt from this rule, which means that they are free to pursue abstract purposes, as long as those purposes be charitable. Charities of course also enjoy, differing from jurisdiction to jurisdiction, certain fiscal advantages. There are also certain advantages to being constituted as a charity from the perspective of data protection law, and we will elaborate more on this later.

There are rules at common law that determine what counts as a charitable purpose. A purpose must fall under one of four 'heads' of charity to count as charitable. These are (1) Education; (2) Religion; (3) Relief of Poverty; and (4) Other Purposes Beneficial to the Public. Some jurisdictions, such as the United Kingdom and Singapore, have enacted legislation or provided non-statutory guidance to specify purposes which fall under (4),[77] but (4) remains an 'open' category in the sense that the courts can recognise new charitable purposes that are sufficiently similar to ones previously recognised.[78]

One other important feature of the charitable trust is that it must (subject to certain statutory exemptions in certain jurisdictions)[79] only pursue charitable purposes. It may not pursue non-charitable purposes. This is closely linked to another

---

77 See, *eg Charities Act 2011* (UK), c 25, s 3.

78 Penner, *Law of Trusts*, *supra* note 20 at paras 14.9-14.16.

79 See, *eg Trustees Act* (Cap 337, 2005 Rev Ed Sing), s 64:

(1) No trust shall be held to be invalid by reason that some non-charitable and invalid purpose as well as some charitable purpose is or could be deemed to be included in any of the purposes to or for which an application of the trust funds or any part thereof is by such trust directed or allowed.

(2) Any such trust shall be construed and given effect to in the same manner in all respects as if no application of the trust funds or any part thereof to or for any such non-charitable and invalid purpose had been or could be deemed to have been so directed or allowed. (This provision does not necessarily allow the application of charity funds to non-charitable purposes, but it does save the charitable trust from invalidity.)

feature—that charities cannot be run for profit, and may only pursue business-related activities that are ancillary to their charitable purposes. (A religious charitable trust would be allowed to run a bake sale to raise funds for the trust, for example.)

The 'education' head of charity includes the carrying out of useful research, and given the fact that digital files record information and can be analysed, this seems to be the most obvious charitable purpose to which a data trust's assets would be devoted. In *McGovern v Attorney-General*,[80] Slade J said:

> A trust for research will ordinarily qualify as a charitable trust if, but only if, (a) the subject matter of the proposed research is a useful subject of study; and (b) it is contemplated that knowledge acquired [thereby] will be disseminated to others; and (c) the trust is for the benefit of the public, or a sufficiently important section of the public. (2) In the absence of a contrary context, however, the court will [readily construe] a trust for research as importing subsequent dissemination of the results thereof. (3) Furthermore if a trust for research is to constitute a valid trust for the advancement of education, it is not necessary either (a) that a teacher/pupil relationship should be in contemplation or (b) that the persons to benefit from the knowledge to be acquired should be [students] in the conventional sense.[81]

The requirement of subsequent dissemination is worth discussing. This requirement is not specific to 'research' charitable trusts—it is common to all charitable trusts that fall under the 'education' head. In *McGovern v AG*, a case which concerned human rights research, the preparation and publication of the results of research, the institution and maintenance of a library accessible to the public for the study of matters connected with the research and the production and distribution of documentary films showing the results of the research were cumulatively held to fulfill the dissemination requirement.[82]

Does the fact that the disseminated information eventually reaches a party who uses the information for profit-making purposes pose a problem? It does not. In *Incorporated Council of Law Reporting for England and Wales v Attorney-General,*[83] it was held that the Incorporated Council of Law Reporting, a company incorporated "for the purpose of recording in a reliably accurate manner the development and application of judge-made law and of disseminating the knowledge of that law"[84] pursued a valid, charitable, educational purpose. The fact the council's publications "helps the lawyer to earn his livelihood" was not fatal to the exclusively charitable character of the council's objects, as it does not detract from the "primary scholastic function of advancing and disseminating knowledge of the law".[85]

The best analogy for a charitable data trust or company is that of a library. A library can be open to the public, or to particular individuals, such as particular researchers

---

80 [1982] 1 Ch 321 [*McGovern v AG*].
81 *Ibid* at 352-353.
82 *Ibid.*
83 [1972] Ch 73.
84 *Ibid* at 103.
85 *Ibid*.

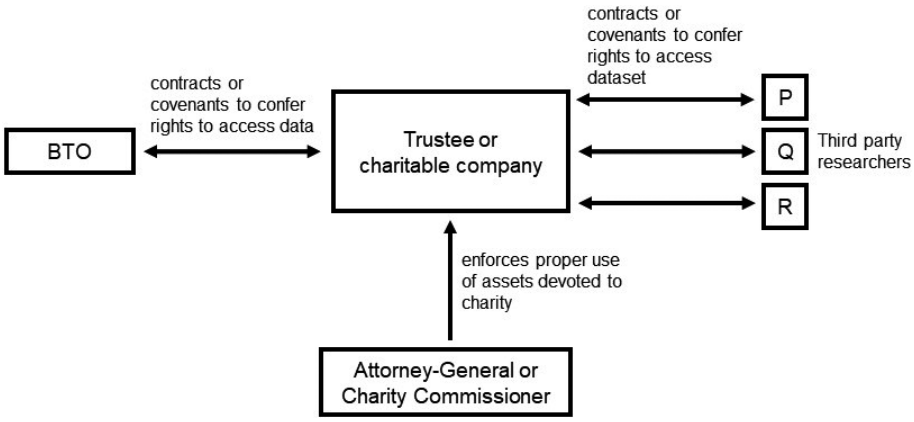


Fig. 3.

whose work will further the educational purpose of the charity.[86] Let us say the British Trust for Ornithology digitises all the data it has collected over the years from birders, and wishes this data to be available for researchers. They could set up a particular charity for research on this data set by sending the data to a charitable trust or company, or giving access rights to the data set to the trust or company in just the same way as with the Telco/Transhub joint venture trust we have already examined. The trustee or company could then grant access rights to researchers on such terms as the trustees might impose to ensure that their efforts would serve the educational or research purpose. See Figure 3.

V. Data Protection Issues Arising In The Creation And Administration Of Data Trusts

The operations of a data trust will necessarily involve the collection, use and/or disclosure of data. If the data in question is *personal* data, then the rules of data protection law will potentially apply. Whether a particular jurisdiction's data protection law applies to the data trust will depend upon the territorial scope of that jurisdiction's data protection law, and it is possible that more than one jurisdiction's data protection law will apply to the operations of the data trust.

A. *Application of Canadian Data Protection Law*

The discussion that follows will assume the application of Canadian data protection laws. Under the PIPEDA, the data trustee and the other organisations involved in the data trust would have to comply with ten fair information principles, among other

[86] Access rights granted to a small number of individuals would not necessarily contravene the dissemination requirement discussed earlier, because the dissemination requirement concerns the dissemination of the results of the research, and not the persons involved in the research.

obligations;[87] similar data protection obligations are found in the provincial data protection laws.[88] Singapore data protection law largely mirrors that of Canada.[89] This paper now proceeds to examine how the data protection obligations may apply to a data trust. It will seek to show that data trusts do not face any significant special problems in terms of compliance with data protection law.

1. *Notice and consent*

When a data trustee accesses personal data pursuant to its use right over that data, what in effect occurs is the disclosure of personal data by the settlors, and the collection and use of personal data by the data trustee. These processes also occur, *mutatis mutandis*, when a third party accesses the personal data. These organisations (that is, the data trustee, settlor and third parties) are generally required under data protection laws to obtain the prior consent of the individuals whose personal data are being collected, used or disclosed.[90] In obtaining consent, organisations are obliged to notify the individuals of the purposes for which their personal data are collected, used or disclosed.[91] The collection, use or disclosure cannot then extend beyond the purposes of which the individuals have been notified and for which their consent has been obtained.[92]

While the rules relating to notice and consent may on occasion be onerous (especially where large data sets involving many individuals are involved), they do not pose difficulties that are peculiar to data trusts. Furthermore, where the data trust is a charitable trust, the organisations participating in the data trust may be well-placed to take advantage of certain exceptions built into Canadian data protection legislation. For example, an organisation may use personal data without the knowledge or consent of the individual, if it is used "for statistical, or scholarly study or research, purposes that cannot be achieved without using the information, the information is used in a manner that will ensure its confidentiality, it is impracticable to obtain consent and the organization informs the Commissioner of the use before the information is used"—this may be relevant to a charitable data trust for education.[93]

2. *Appropriate purposes*

There is a separate requirement that organisations only collect, use or disclose personal data for "purposes that a reasonable person would consider are appropriate in the circumstances".[94] The appropriateness of the purposes of a particular collection, use or disclosure is assessed in the light of the circumstances which include,

---

87 *PIPEDA*, *supra* note 32, s 5(1).

88 Namely the *ABPIPA* (*supra* note 35) and *BCPIPA* (*supra* note 35). These have been established to be substantially similar to the *PIPEDA* (*ibid*) pursuant to *PIPEDA*, s 26(2)(b).

89 Singapore's data protection law is primarily constituted by the Personal Data Protection Act 2012 (No 26 of 2012, Sing) [*PDPA*].

90 *PIPEDA*, *supra* note 32, Schedule 1, para 4.3; *PDPA*, *supra* note 32, s 13.

91 *PIPEDA*, *ibid*, Schedule 1, para 4.3.2; *PDPA*, *ibid*, s 14(1)(a). This is to ensure that the consent is informed.

92 *PIPEDA*, *ibid*, Schedule 1, paras 4.4 and 4.5; *PDPA*, *ibid*, s 18(b).

93 *PIPEDA*, *ibid*, s 7(2)(c). See also *PIPEDA*, s 7(3)(f) for a similar exemption for disclosures. Singapore has similar exemptions: *PDPA*, *ibid*, Third Schedule, para 1(i) and Fourth Schedule, para 1(q).

94 *PIPEDA*, *ibid*, s 5(3); *PDPA*, *ibid*, s 18(a).

according to the Office of the Privacy Commissioner ("OPC"): (a) the degree of sensitivity of the personal data; (b) whether the organisation's purpose represents a legitimate need or bona fide business interest; (c) whether the collection, use or disclosure would be effective in meeting the organisation's needs; (d) whether there are less invasive means of achieving the same ends at comparable cost and with comparable benefits; and (e) whether any loss of privacy is proportionate to the benefits gained.[95] The OPC has also identified a number of "No-Go Zones", which are purposes for which the collection, use or disclosure of personal data would generally be considered inappropriate.[96]

It may be suggested that, where the data trust is a charitable trust, its purposes for collecting, using or disclosing personal data are likely to be considered appropriate by a reasonable person. Epidemiological research conducted by a charitable data trust for education, for example, could hardly be contended to be an objectionable purpose for the collection, use or disclosure of personal data.[97] It must be said, however, that there is no guarantee that *all* the collection, use and disclosure of personal data by organisations as part of a charitable trust would be regarded as compliant with the appropriate purpose requirement, as the particular circumstances of each instance of collection, use or disclosure must be considered. Also, the fact that the organisation is participating in a charitable data trust does not, by itself, affect the assessment of the appropriateness of its purpose for its collection, use or disclosure of personal data.

3. *Other data protection obligations*

Apart from the abovementioned obligations that pertain to the collection, use and disclosure of personal data (namely the obligations to notify individuals and obtain their consent, and to ensure that the purposes for the collection, use or disclosure are appropriate), there are other obligations that Canadian data protection law imposes on organisations. Some of the other main obligations that the organisations of a data trust would need to fulfil include: (a) the designation of individuals who are accountable for the organisation's data protection compliance;[98] (b) the implementation of data protection policies and practices;[99] (c) ensuring the accuracy of personal data;[100] (d) taking appropriate data security safeguards;[101] (e) providing transparency to individuals about the organisations' data protection policies and

---

95 Office of the Privacy Commissioner of Canada, Guidance on inappropriate data practices: Interpretation and application of subsection 5(3), online: Office of the Privacy Commissioner of Canada <https://www.priv.gc.ca/en/privacy-topics/collecting- personal-information/consent/gd_53_201805/> [*OPC Section 5(3) Guidelines*]. See also *Turner v Telus Communications Inc* [2005] FCJ 1981 at para 48.

96 *OPC Section 5(3) Guidelines*, *ibid*.

97 Further, there is an argument that if a purpose (such as research) has been expressly listed as an exemption for the requirement of notice and consent, such a purpose has implicitly been endorsed by legislature, and is therefore a generally appropriate purpose for the collection, use and disclosure of personal data: see Order P2008-008: United Food and Commercial Workers, Local 401 (Re), [2009] CanLII 90942 at para 98.

98 *PIPEDA*, *supra* note 32, Schedule 1, para 4.1.1; *PDPA*, *supra* note 32, s 11(3).

99 *PIPEDA*, *ibid*, Schedule 1, para 4.1.4; *PDPA*, *ibid*, s 12(a).

100 *PIPEDA*, *ibid*, Schedule 1, para 4.6.1; *PDPA*, *ibid*, s 23.

101 *PIPEDA*, *ibid*, Schedule 1, para 4.7.1; *PDPA*, *ibid*, s 24.

practices;[102] (f) granting individuals access to, and the ability to correct, their personal data;[103] and (g) addressing individuals' challenges or complaints.[104]

Again, while these obligations may be onerous, they are not made more onerous by the organisations' participation in a data trust. On the contrary, if the settlors' data sets are entirely deposited with the data trustee (that is, the settlors do not retain any copy of the data sets), the settlors may free themselves of the burdens of compliance with the abovementioned data protection obligations, leaving the data trustee to manage all their data sets; in that situation, only the costs of a single data management system, maintained by the data trustee, need to be incurred.[105]

B. *Application of European Data Protection Law*

It will be useful to consider, briefly, how the GDPR might apply to a data trust that falls within the material and territorial scope of the GDPR. Unlike the PIPEDA which creates a single data protection framework that regulates the conduct of "organisations", the GDPR creates a bifurcated system that regulates entities differently depending on whether they qualify as "controller" or "processor". When assessing how data protection responsibilities are allocated among the entities participating in the data trust, it will therefore be of first importance to determine whether those entities constitute controllers or processors under the GDPR.

A "controller" is an entity who "alone or jointly with others, determines the purposes and means of the processing of personal data";[106] according to the Article 29 Working Party, a controller is the entity who has the factual influence to determine the purposes and means of processing, and this factual influence is assessed by reference to the legal and factual circumstances.[107] On the other hand, a "processor" is an entity who merely "processes personal data on behalf of the controller".[108]

Controllers and processors have different obligations under the GDPR. Generally speaking, controllers are subject to a broader range of responsibilities than processors.[109] Where personal data is processed, the GDPR stipulates that the controller is responsible for implementing "appropriate technical and organisational measures to ensure and to be able to demonstrate" that the processing is done in accordance with the GDPR.[110] The controller is also responsible for implementing measures to achieve data protection by design and by default,[111] and to conduct data protection impact assessments in the event that processing is likely to result in "a high risk to the

---

[102] *PIPEDA*, *ibid*, Schedule 1, para 4.8.1; *PDPA*, *ibid*, s 12(d).

[103] *PIPEDA*, *supra* note 32, Schedule 1, para 4.9.1; *PDPA*, *supra* note 89, ss 21 and 22.

[104] *PIPEDA*, *supra* note 32, Schedule 1, para 4.10.1; *PDPA*, *ibid*, s 12(b).

[105] This "concentration" of data is, of course, also possible without a data trust.

[106] *GDPR*, *supra* note 29, art 4(7).

[107] Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"*, 00264/10/EN WP 169 (2010) at 9.

[108] *GDPR*, *supra* note 29, art 4(8).

[109] That said, there are some obligations that are common to both controllers and processors. These include the obligation to maintain records of data processing activities (*GDPR*, *ibid*, art 30), the obligation to "implement appropriate technical and organisational measures" to secure personal data (*GDPR*, *ibid*, art 32), and the obligation to designate data protection officers under certain specified circumstances (*GDPR*, *ibid*, art 37).

[110] *GDPR*, *ibid*, art 24.

[111] *GDPR*, *ibid*, art 25.

rights and freedoms of natural persons".[112] Furthermore, the rights of data subjects as provided for in Chapter III are largely framed as rights against the controller.[113]

It is unfortunately not possible to state, in the abstract, whether any entity participating in a data trust will be a controller or processor, and this is because the circumstances surrounding each data trust must be taken into account. Thus, for instance, it is not possible to come to the categorical conclusion that all data trustees are necessarily controllers, because whether any particular data trustee qualifies as a controller over a set of personal data would depend on a number of circumstances, including the precise terms of the data trust to which the data trustee is bound, the terms of the contracts conferring the use rights that constitute the subject matter of the data trust, the practical arrangements that the settlors and the data trustee have developed to grant the data trustee access to the personal data, and how the data trustee actually deals with the personal data. Put simply, if the data trustee exercises some degree of control over how and why the personal data is processed, then it is likely to be a data controller; if, on the other hand, it simply processes the personal data strictly pursuant to the instructions of the settlors, then it is likely to be a data processor.

C. *Conflicts between Trustee Duties and Data Protection Obligations*

An issue specific to the data trustee should be addressed here. It is clear that if a data trustee processes personal data in the operation of the data trust, then it will simultaneously bear obligations under data protection law and trust law. Are there situations where there is a conflict between the data trustee's data protection obligations and its trustee duties? How are such conflicts resolved?

One situation where there may be a clash between the data trustee's data protection obligations and its duties as a trustee may be suggested by an example. The terms of the data trust may require the data trustee to manage and exploit personal data in the data sets of the data trust for the purposes of research in some defined field; this would almost certainly require the data trustee to use or disclose the personal data. As a trustee, the data trustee is required to comply with the terms of the data trust. However, it may happen that the individuals whose personal data forms part of the data trust's data sets withdraw their consent to the use and disclosure of their personal data, and in that event the data trustee is generally obliged, under data protection law, to respect the individuals' withdrawal and cease to use or disclose their personal data.[114] In this situation, the data trustee is required by the terms of the data trust to use and disclose personal data, but prohibited from doing so by the rules of data protection law.

There are also situations where the data trustee is required to destroy the personal data within the data trust's data sets, and this may, at first glance, appear to come into conflict with the data trustee's duty to preserve the trust assets. The PIPEDA provides

---

[112] *GDPR*, *supra* note 29, art 35.

[113] These rights include the rights of transparency, access, rectification, erasure, restriction of processing, data portability, and objection.

[114] *PIPEDA*, *supra* note 32, Schedule 1, para 4.3.8; *PDPA*, *supra* note 89, s 16. *GDPR*, *supra* note 29, art 7(3). The GDPR also separately confers on data subjects the right to restrict processing and the right to object to processing: see *GDPR*, arts 18 and 21.

for a requirement to limit retention of personal data, under which organisations are obliged to destroy, erase, or make anonymous any personal data that is no longer required to fulfil the purposes for which the personal data was collected.[115] GDPR imposes a similar requirement under Article 5(e).[116] The GDPR also confers on individuals the right to have their data erased, assuming certain conditions specified in Article 17 are met.[117]

While the situations stated above may appear to generate a conflict between a data trustee's data protection obligation and its duties *qua* trustee, we submit that there is no real conflict, or rather, that this sort of 'conflict' is not peculiar to data trusts and the regulation of data under data protection laws. In the first place, a data trust, like any other type of express trust, would be subject to the doctrine of illegality. The data trust cannot validly oblige the data trustee to commit an illegal act—to the extent that the data trust purports to do so, it is void. So, for example, if a term of the data trust purports to oblige the data trustee to process personal data for illegal purposes, the data trustee is bound not to carry out that term of the data trust. The data protection obligations of a data trustee override its trustee duties, and in the event that there is any conflict between the data protection obligations and the trustee duties of the data trustee, the former prevails.

More generally, the trustee receives whatever trust property he does, 'warts and all'. So, for example, an English trust may hold title to land in France, but in certain respects this is a 'flawed' trust asset, because the beneficiaries may have difficulty enforcing the trust over land held in a jurisdiction that does not recognise trusts.[118] The same lesson applies here. The data trustee receives trust data subject to all the general rules that govern this kind of asset, just as a trustee who owns title to land is bound by the law preventing owners from using the land so as to create a nuisance.

VI. Conclusion

In this paper we have dispelled some uncertainties and confusions about data trusts. In particular we have shown that the device of the trust, on traditional equitable principles of trust law, is a perfectly suitable vehicle for the management of data for both private and public purposes. Rights to data are suitable trust assets, and the data protection laws do not raise any particular problems specific to data trusts or data trustees as holders and handlers of rights to data.

---

115 *PIPEDA*, *ibid*, Schedule 1, para 4.5.8; *PDPA*, *ibid*, s 25.

116 Article 5(e) requires that personal data be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed", but does permit a longer storage period "insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes".

117 *GDPR*, *supra* note 29, art 17. For example, one ground for erasure is where the personal data is "no longer necessary in relation to the purposes for which they were collected or otherwise processed". In Canada there is no such right to erasure, but it would appear from a recent public consultation that the Canadian Government is contemplating including the right to erasure into the *PIPEDA*. See Government of Canada, *Strengthening Privacy for the Digital Age,* online: Government of Canada <https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html>.

118 See Penner, *Law of Trusts*, *supra* note 20 at para 2.117.