DOES THE DEFINITION OF "PROPERTY" IN THE CRIMES ACT 1961 INCLUDE ELECTRONICALLY STORED DATA?

THE COMPUTER SAYS "NO".

LANCE GREEN

A dissertation submitted in partial fulfilment of the degree of Bachelor of Laws (Honours) at the University of Otago, Dunedin, New Zealand

October 2015

ACKNOWLEDGEMENTS

This dissertation owes much to the people acknowledged below. Any faults or omissions, however, remain mine and mine alone.

To my supervisor, Margaret Briggs, thank you for taking a genuine interest in this work and for your guidance throughout the course of the year. Your comments and suggestions provided much-needed direction.

To David Eyers, thank you for your thorough and lucid explanations of how a computer works. As someone whose technological know-how is sometimes surpassed by my octogenarian grandmother, your input was critical to my understanding of my topic.

To Jesse Wall, thank you for your helpful comments both at my seminar and in subsequent discussions regarding the concept of property. You helped make writing this dissertation a fascinating challenge.

To Stephen Mackereth and Mike Scott, thank you for trading ideas with me. You helped refine and clarify my thoughts.

Finally to my parents, to whom I will be eternally indebted, I cannot articulate how grateful I am to you for everything, including suffering through various drafts of this work.

TABLE OF CONTENTS

INTRODUCTION

In September 2011, the English national rugby side was touring New Zealand as part of its participation in the Rugby World Cup. The captain of the side was Mike Tindall, who had recently cemented his status as a public figure in Britain by marrying the Queen's granddaughter. Unfortunately for Mr Tindall, a night out in a Queenstown bar saw an incident between him and a female patron captured on CCTV footage. Jonathan Dixon, a bouncer employed by the bar, obtained a copy of the footage, which the Crown alleged he planned to sell to the British tabloids. In any event, Mr Dixon did not sell the footage to the press and ended up posting the footage on a video-sharing site, generating a publicity storm in both New Zealand and the United Kingdom.[1] Mr Dixon was then successfully prosecuted in the District Court under s 249 of the Crimes Act 1961 for dishonestly accessing a computer to obtain "property".[2] The property in question was deemed to be the digital file containing the footage, which Mr Dixon had obtained from one of the bar's work computers.[3] The case reached the Court of Appeal, which held that a digital file does *not* qualify as "property" for the purposes of the Crimes Act.[4] Instead, Mr Dixon was convicted under s 249 for dishonestly accessing a computer to obtain a "benefit".[5] Mr Dixon subsequently obtained leave to appeal to the Supreme Court.[6] The approved question encompassed whether the Court of Appeal was correct to hold that the CCTV files are not property.[7] At the time of writing, the Court had not released its judgment.

The central thesis advanced in this dissertation is that the Court of Appeal was correct to hold that the criminal definition of "property" does not extend to electronically stored data. The Court of Appeal reached its conclusion on the basis that electronic data could

[1] For a summary of the facts see *Dixon v R* [2014] NZCA 329, [2014] 3 NZLR 504 at [4]-[8].
[2] *R v Dixon* DC Invercargill CRI-2011-059-1122, 2 August 2013.
[3] Ibid at [13]-[14].
[4] *Dixon*, above n 1.
[5] Crimes Act 1961, s 249(1)(a).
[6] *Dixon v R* [2014] NZSC 151. The case was heard on 24 March 2015. For the official transcript see *Dixon v R* [2015] NZSC Trans 9; SC 82/2014.
[7] *Dixon*, above n 6, at [1].

not be meaningfully distinguished from "pure information",[8] which the common law does not recognise as property.[9] Accordingly, the following statement is the critical proposition on which the Court's conclusion rests:

> Electronic footage stored on a computer is indistinguishable in principle from pure information.[10]

Throughout the common law world, courts have rejected the idea that information is property. Thus, in the words of the Court: "if confidential information is not property digital footage also cannot be."[11] This dissertation does not challenge the common law orthodoxy that information is not property. Rather, the ambition of this dissertation is to critically analyse the equation of electronic data with pure information. Accordingly, the wider question of whether pure information should qualify as property is not the question under scrutiny.

In defending the equation of electronic data with pure information in the context of the Crimes Act, this dissertation analyses the concept of property, the relevant statutory context and the legitimate objectives of the criminal law. It is argued that all three of these suggest electronic data is appropriately equated with pure information and therefore excluded from the criminal definition of "property". The following framework organises these lines of analysis.

Chapter I examines the definition of "property" in s 2 of the Crimes Act. The key point of this chapter is to show that the criminal definition of "property" maps on to antecedent property concepts fashioned by the civil courts. The critical consequence

[8] The court referred to "pure information" to distinguish general information from "digital information". When this dissertation refers to "pure information" it is referring to information in its general sense and *not* to electronic data.
[9] *Dixon v R* above n 1 at [31]. As authority for the proposition that information is not property the court cited: *Oxford v Moss* (1979) 68 Cr App R 183; *Stewart v R* [1988] 1 SCR 963; *Money Managers Ltd v Foxbridge Trading Ltd* HC Hamilton CP67/93, 15 December 1993; *Taxation Review Authority* 25 [1997] TRNZ 129; *Boardman v Phipps* [1966] UKHL 2, [1967] 2 AC 46; *Hunt v A* [2007] NZCA 332, [2008] 1 NZLR 368; and *Farah Constructions Pty Ltd v Say-Dee Pty Ltd* [2007] HCA 22.
[10] *Dixon*, above n 1, at [31].
[11] Ibid at [32].

of this argument is that a conceptual analysis of property must accompany an exercise in statutory interpretation.

Chapter II examines the concept of property. The aim of this chapter is to assess the compatibility of electronic data with the concept of property. Accordingly, the concept of property is analysed with specific reference to the argument that electronic data can be distinguished from pure information on the basis of its physical existence. This chapter rejects that argument and concludes that conceptual analysis supports the equation of electronic data to pure information.

Chapter III engages in statutory interpretation. This chapter analyses the relevant legislative history and context in order to assess the various legal arguments that can be made in favour of including a computer file within the criminal definition of "property". Ultimately, this chapter concludes that the relevant legislative context and history support the equation of electronic data to pure information.

Finally, chapter IV considers the various consequences that ensue if computer data is not included within the Crimes Act's definition of property. This chapter aims to articulate the legitimate grounds for criminalising computer misuse in order to see whether the exclusion of digital data from the criminal definition of "property" is desirable from a policy perspective. This chapter concludes that the exclusion of digital data from the criminal definition of "property" accords with the appropriate policy concerns underlying the criminalisation of computer misuse.

CHAPTER I

THE CRIMINAL DEFINITION OF "PROPERTY"

A Overview

In this chapter, it is argued that the criminal definition of "property" maps on to antecedent property concepts that have been constructed by the civil courts. The definition of "property" in s 2 must be seen, therefore, as an incorporative definition that delegates, to a certain extent, to the law of property. Nevertheless, this chapter also argues that despite its breadth, the criminal definition of "property" also takes its shape from its context. Thus, it is argued that the admission of something into the criminal definition of "property" must accord with the underlying purposes of the Crimes Act.

B A wide definition of "property"

The Crimes Act has the following definition of "property":

> **Property** includes real and personal property, and any estate or interest in any real or personal property, money, electricity, and any debt, and any thing in action, and any other right or interest.[12]

The first thing to note about the definition is its circularity. The first clause of the definition is simply that "property includes real and personal property". This clause merely reflects the fact that there are only two types of private property.[13] The term "real property" refers to land while the term "personal property" refers to both tangible property like chattels and intangible property such as choses in action.[14] Thus, the phrase "real and personal property" covers all possible types of private property. The

[12] Crimes Act, s 2.
[13] Sarah Worthington *Equity and Property: Fact, Fantasy and Morals* (University of Queensland Press, Queensland, 2009) at 6.
[14] A "chattel" is a physical object or 'thing'. A "chose in action", on the other hand, is essentially the right to sue. A debt is an example of a chose in action. Accordingly, a chose in action is a legal construct and has no existence in the physical world. That is why some definitions of "property" refer to both "tangible" and "intangible" property. See, for example, the Property Laws Act 2007, s 3.

clause must be seen, therefore, as tautological because it basically says: "property includes property". The second thing to note about the definition is its inclusive nature. Section 2 defines "property" to *include* various things, rights and interests. It is not, therefore, an exhaustive definition of "property". Accordingly, the definition of "property" in the Crimes Act does not actually provide the materials necessary to determine whether something qualifies as property without reference to the general law.

Plainly, it is not possible for the definition of "property" in s 2 to provide an exhaustive catalogue of the things that qualify as property. As a result, the criminal definition of "property" has been drafted to reflect the *concept* of property. Chapter II explores the concept of property in greater depth but for present purposes it suffices to make a crucial point: property law does not actually concern itself with 'things' but rather 'rights to things'.[15] Accordingly, referring to an object as an item of "property" is merely shorthand for the fact that the particular object in question is capable of attracting property rights.[16] Regularly, the various property rights operating in respect of a property item are parcelled out amongst a host of different people. Thus, the reference in s 2 to "any other right or interest" reflects the fact that multiple people can possess property rights in respect of the same thing. That Part 10 of the Crimes Act is designed to reflect the rights-based nature of property law is made clear by its heading: "crimes against *rights* of property".[17] In addition, it is sometimes the case that a property item *is* a particular right itself rather than an object. For example, a "debt" is the right to recover a certain amount of money. The right to recover *is* the item of property.[18] Accordingly, the definition of "property" refers to "any debt" and "any thing in action" to reflect this.

The foregoing analysis demonstrates that the definition of "property" in s 2 must be understood as reflecting the concept of property, which has been developed by the civil courts. It does not aim, therefore, to provide a self-contained or exhaustive definition for property. Rather, it aims to reflect the concept of property by protecting a wide

[15] See generally Bruce Ackerman *Private Property and the Constitution* (Yale University Printing Press, New Haven, London, 1977) at 26-27. There is fuller discussion on this point on pages 10-11.
[16] This dissertation often refers to "property". This is a far more convenient term than the more legally precise: "a particular thing that is capable of attracting property rights". Nevertheless, the reader should understand the term "property" as being shorthand for that more convoluted phrase.
[17] Crimes Act, Part 10 heading (emphasis added).
[18] Intellectual property rights are another example of property items that exist only as rights.

category of people who may have property rights in respect of a wide category of things. Thus, it is not possible to conclusively determine what things qualify as "property" without recourse to sources of law external to the Crimes Act itself.

C A specific definition of property for the Crimes Act?

Although, it is clear that the criminal definition of "property" refers to civil law property concepts, a more difficult question asks whether all civil law property items necessarily qualify for the criminal law as well. The critical question arising here is whether the concept of property has "remained unified or become fractured" due to its development in different contexts.[19] Michael Hostetler has labeled these two theoretical positions the "pragmatist's universe" and the "idealist's universe".[20] In the pragmatist's universe, the perceived differences in policy considerations underlying different statutes produce different visions of property.[21] On the other hand, in the idealist's universe, there is a single vision of property because "basic fairness and preservation of a legal system's legitimacy ensure that concepts of property do not differentially evolve".[22]

The argument for a specific definition of property posits that the aims of a particular field of law will largely determine whether something qualifies as property for the purpose of that field of law. On this basis, the definition of property in the Crimes Act should be seen as specialised for the purposes of the criminal law. Stuart Green, for example, has argued that: "we need to consider both the goals (and consequences) of each branch of law and the underlying concerns that color the 'propertization' of such things on their own terms."[23] In similar vein, Weinrib has argued that the "web of legal relations" comprising property takes "its shape from its context" and that "civil and criminal contexts can be very different."[24]

---

[19] Michael J. Hostetler "Intangible Property Under the Federal Mail Fraud Statute and the Takings Clause: A Case Study." (2000) *Duke LJ*. 589 at 590-591.
[20] Ibid.
[21] Ibid, 590.
[22] Ibid, 590-591.
[23] Stuart Green, *13 Ways to Steal a Bicycle* (Harvard University Press, Cambridge, Massachusetts, 2012) at 206.
[24] Arnold S. Weinrib "Information and Property" (1988) 38 *U.T.L.J.* 117 at 137.

The Canadian Supreme Court espoused this view in the case *Stewart v R*.[25] In that case, the Court had to decide whether confidential information qualified as property for the purposes of the criminal law. The Court reasoned that even if confidential information were to be considered as property under civil law, "it would not automatically follow that it qualified as property for the purposes of criminal law."[26] The Court also argued that the fact something is not property under civil law is likewise not conclusive for the purpose of criminal law.[27] The Court made a number of arguments in defence of this proposition.

First, the Court noted that the characterisation of something as property triggers a series of legal consequences. The consequences of characterisation differ in the criminal and civil contexts.[28] According to the Court in *Stewart*, it is necessary to consider whether the consequences following on from the inclusion of something into the criminal law's definition of "property" accord with the objectives of criminal law. The Court noted that including information within the criminal definition of "property" could have unfortunate results. For instance, any person who came into possession of information knowing it to be unlawfully obtained could face liability as a receiver for as long as memory permitted retention of the information.[29] Presumably, it is concerns such as these that led Elias CJ to express fears that an overly broad definition of property in the context of the New Zealand Crimes Act could result in over-criminalisation.[30]

Secondly, the Court in *Stewart* identified the different interests that are at stake in the civil law as opposed to the criminal law.[31] In civil litigation, the courts simply have to balance the interests of the parties involved whereas the criminal law is designed to prevent wrongs against society as a whole.[32] Accordingly, whether something should be given proprietary protection in the context of the criminal law requires "a weighting of interests much broader than those of the parties involved."[33] On this analysis, classification of something

[25] *Stewart v R* above n 9.
[26] Ibid at [25].
[27] Ibid.
[28] Ibid at [27].
[29] Ibid.
[30] *Dixon v R*, above n 6, at pages 46 and 58. In the course of oral arguments, Elias CJ expressed concerns of over-criminalisation resulting from an "all-encompassing" definition of "property".
[31] At [28].
[32] See below n 195. There is fuller discussion on this point in Chapter IV.
[33] At [28].

as property for the criminal law requires a justification pertinent to the overall interests of society as a whole.

D Conclusion

There are two important conclusions to draw from this chapter. First, it must be recognised that the criminal definition of "property" takes its colour from the general law. The definition of "property" in the Crimes Act is drafted widely and does not expressly narrow the concept of property in any way. Accordingly, whether something qualifies as property in the general law will be very relevant to whether it qualifies as property in the criminal context. As a result, this dissertation analyses the concept of property and reviews other statutes with "property" definitions in order to assess whether the general law treats digital data as property. Second, the criminal definition of "property" must also be interpreted with regard to the relevant provisions and purposes of the Crimes Act.[34] Accordingly, this dissertation assesses whether the exclusion of computer data from the definition of "property" in s 2 of the Crimes Act is consonant with the purposes of the criminal law.

[34] Note that some commentators have taken a contrary position. See Bruce Robertson and Jeremy Finn (eds) *Adams on Criminal Law 2014 Student Edition* (Thomson Reuters, Wellington, 2014) at CA2.29.01: "[the criminal definition of property] provides a wide definition for the term "property" which includes land and *all* forms of personal property" (emphasis added); Hostetler, above n 19, at footnote 224: "a consistent definition […] ensures that a person is aware of what actions are considered criminal."

CHAPTER II

THE CONCEPT OF PROPERTY AND THE NATURE OF ELECTRONIC DATA

A Overview

The aim of this chapter is to assess whether it is conceptually possible for property rights to inhere in computer files as distinct from the pure information contained on them. Accordingly, this chapter examines the *concept* of property in order to identify the defining features of property rights. This chapter then considers the argument that a computer file can be differentiated from pure information on the basis of a physical existence. It is ultimately concluded that computer data should be equated with pure information in order to conform to a coherent concept of property.

B The concept of property

1. Property is a policy decision

It is critical to first appreciate that the decision to admit a particular right to the category of property is one of policy.[35] As Weinrib observes, our social institutions, including the institution of property, "exist to further certain ends."[36] Accordingly, social and political considerations will often dictate whether or not a particular right acquires the legal status of "property".[37] In other words, if property rights are assigned "the expectation must be that such an assignment will achieve a more desirable result than

[35] Weinrib, above n 24, at 121. See also Sam Ricketson "Confidential Information - A New Proprietary Interest? Part II (1977) *M.U.L.J* 289 at 306-307; *Stewart v The Queen* [1988] 1 SCR 963 (SCC) [28]-[33]; Laura Underkuffler, *The Idea of Property: Its Meaning and Power* (Oxford University Press, Oxford 2003) 11; and Worthington, above n 13, at 8-9: "the classification of resources as property that can be owned by individuals is a matter of choice, not inevitability. The law's changing perception of what is property and what is not reflects the contemporary balance between commercial and economic demands, and social and moral constraints that society is prepared to condone."

[36] Weinrib at 121.

[37] Worthington, above n 13, at 6: "the boundary between property rights and personal rights is never defined. It subject to revision according to social and political norms."

what would otherwise be the case."[38] The law of property is thus purposive. Consequently, just because a right is capable of being proprietary does not mean that it should be.[39] In the case of pure information, policy concerns regarding society's access to information have precluded its admission to the category of property in the common law world.[40] Nevertheless, the point of the following analysis is to illustrate that some things are simply incompatible with the law's conception of property in the first place.

2. Rights not 'things'

It is illuminating to first consider the goal of property law. Put simply, the goal of property law is to regulate the use of resources or 'things'.[41] Property law recognises that 'things' can be used in a variety of ways by a variety of different people. Thus, articulated precisely, the goal of property law is to organise the various ways that rights to use things may be parceled out amongst a host of competing users.[42] To achieve this goal, the law of property concerns itself, not with things *per se*, but with various *rights* that operate in respect of things.[43] This is what enables a host of potential users to organise the use of a particular resource. Co-ownership of a horse, for example, might divide ownership rights ½: ¼: ¼ whereas a more sophisticated strategy might allow different parties to have different *types* of interest in the same asset.[44] It is the rights-based nature of property that has allowed the common law to split ownership and

---

[38] Above n 36.
[39] For example, Canadian and U.S. legislators specified during the Prohibition era that no property rights were to exist in alcoholic beverages. The purpose of the legislation was to discourage commercial transactions in liquor. On this point see Weinrib, above n 24, at 137-139.
[40] There is a fuller discussion on these policy considerations in Chapter IV.
[41] This articulation of property law's "goal" is deliberately broad. There have been a host of justificatory theories advanced in support of private property. Each of these theories advocates property rights on a different normative basis. Nevertheless, all of these theories concern the use of resources. An in-depth discussion of the normative theories advanced in support of private property is beyond the purview of this dissertation. For a concise summary of the philosophical theories advanced in support of private property see Lawrence Becker *Property Rights: Philosophical Foundations* (Routledge and K. Paul, London, Boston, 1977) at 99-103. For a comprehensive review of the justifications for private property see Jeremy Waldron *The Right to Private Property* (Oxford University Press, New York, 1988).
[42] Ackerman, above n 15, at 26.
[43] An early explanation of property as relations among people with respect to things was given by Hohfeld: see Wesley Newcomb Hohfeld, *Fundamental Legal Conceptions as Applied in Judicial Reasoning*, ed. Walter W Cook and foreword Arthur L. Corbin (Greenwood Press, Westport, 1978 [1919]. For a more recent articulation of the rights-based nature of property see: A.M. Honoré, "Ownership," in A.G. Guest, ed. *Oxford Essays in Jurisprudence (First Series)* (Clarendon Press, Oxford, 1961), at 107-47.
[44] Worthington at 16.

possession of tangible assets between different parties.[45] In this way, the disaggregation of 'things' into numerous property rights has allowed the use of resources to be regulated by private actors in sophisticated and complex ways. Thus, in the words of Bruce Ackerman:

> "the fact (or is the law?) of the matter is that property is not a thing, but a set of legal relations between persons governing the use of things."[46]

It remains to be determined, however, what distinguishes a proprietary right from other rights. The following features have been recognised as crucial to the concept of property.

3. Enforceability of the rights against parties not in privity

A crucial feature of property rights is that they are enforceable against a party not in contractual relations with the party seeking to rely on it.[47] This is what differentiates a property right from a mere contractual right. This feature overlaps with the concept of 'excludability' in that a right is said to be proprietary "if it entitles the owner to exclude third parties from interfering with the right."[48] Professor Jackson has gone as far as to suggest that the *"determinative"* feature of property is the availability of a remedy of one kind or another against a party not in privity.[49] The enforceability of the right against an open-ended set of people is certainly an indispensable feature of property but it is not "determinative". This is because the law affords individuals rights with universal application in other non-proprietary contexts.[50] The right to bodily integrity,

---

[45] Ibid.
[46] Ackerman, above n 15, at 26-27.
[47] See Samuel Ricketson, above n 35, at 307-308 and David Jackson *Principles of Property Law* (Law Book Co, Sydney, Melbourne, 1967) at 23 ff.
[48] Worthington at 35. However, "enforceability" cannot be perfectly equated with "excludability" because "enforceability" means only that a remedy is available. In some cases, this may mean recovery *in specie* but it also covers injunctive, declaratory and monetary relief. Thus, with chattels, a plaintiff's remedy is usually in damages for conversion rather than specific restitution and in the case of a restrictive covenant, a court of equity may refuse injunctive relief and instead award damages. Accordingly, powers of exclusion are not perfectly enforced by the courts but are reinterpreted to give them pragmatic expressions: see Ricketson, above n 35, at 308.
[49] Above n 47.
[50] Arianna Pretto-Sakmann *Boundaries of Personal Property: shares and sub-shares* (Hart Publishing, Portland, 2005) at 98: "instances of rights available generally are the right to reputation and bodily integrity."

for instance, manifests itself in the legal right to be free from unwanted contact from other people. To give effect to this right, the tort of battery protects against the intentional application of force to the body of another person without that person's consent or lawful justification.[51] Similarly, the right to privacy is a legal right exercisable against the world at large.[52] These are legal rights exercisable against an open-ended set of people but the rights are not proprietary in nature.

Further examples can be found in legislation. Every person is afforded the right to be free from discrimination by s 19 of the New Zealand Bill of Rights Act.[53] Similarly, s 14 of the Bill of Rights Act affords every New Zealand citizen the right to free speech.[54] Although the Act only applies to acts done by persons or bodies in pursuit of a public function,[55] these rights are still actionable against parties in the absence of contractual relationships. These rights, however, are not property rights. As can be seen, therefore, enforceability of a right against a party not in privity does not provide a complete answer. It is necessary, therefore, to identify some other defining features of property.

4. Separability[56]

A defining characteristic of property rights is that they exist independently of the rights-holder. As James Penner has written: "only those 'things' in the world which are contingently associated with any particular owner may be the objects of property."[57] In other words, the holding of a property right is *contingent* on some event that vests the right in an individual. On the other hand, non-contingent rights, such as the right to free speech or the right to be free from unwanted contact, are not contingently

[51] Stephen Todd (ed) *The Law of Torts in New Zealand* (5th ed) (Brookers, Wellington, 2009) at 99 citing *P v T* [1998] 1 NZLR 257 (CA).
[52] In New Zealand, the tort of privacy has two elements: (1) the existence of facts in respect of which there is a reasonable expectation of privacy; and (2) publicity given to those private facts would be considered highly offensive to an objective reasonable person: *Hosking v Runting* [2004] NZCA 34, [2005] 1 NZLR 1. The Privacy Act 1993 also protects the right to privacy in the context of personal information.
[53] New Zealand Bill of Rights Act 1990, s 19.
[54] New Zealand Bill of Rights Act 1990, s 14: "everyone has the right to freedom of expression, including the freedom to seek, receive, and impart information and opinions of any kind in any form."
[55] New Zealand Bill of Rights Act 1990, s 3.
[56] James Penner *The Idea of Property in Law* (Clarendon Press, Oxford, 1997). See in particular Chapter 5, pages 105-128.
[57] Ibid at 111.

associated with a particular owner.[58] Rather, the possession of these rights is a direct consequence of citizenship. Expressed another way, individuals are *entitled* to their personal rights; they *have title* to their property.[59]

It is possible to test whether a right is contingent by "asking whether a subsequent rights-holder is able to stand in the same position with regards to the resource as the initial rights-holder."[60] In other words, no normative consequences beyond mere allocative consequences should accompany the transfer of property rights.[61] In contrast to the transfer of property rights, a host of normative consequences would attend the transfer of personal rights such as the right to privacy or the right to freedom of expression. Transferring those rights would not merely reallocate the use of some 'thing' but rather reshape the complexion of an individual's relationship with the rest of society.

A thorough exposition of this particular feature is unnecessary because electronic data easily satisfies the separability thesis. A digital file (comprised of electronic data) is clearly contingently associated to its user. No one is naturally 'entitled' to a digital file. Rather, an individual comes into possession of a digital file *because* of some event, such as the creation or purchase of the file. Thus, the transfer of a digital file does not trigger any normative consequences beyond mere allocative ones.

5. Transferability of the rights

A logical consequence of separability is the ability to transfer. In other words, if rights exist independently of a person then they are assignable or transferable to another person. Thus, as Munzer points out, *personal* rights are rights that protect interests or choices other than the choice to transfer whereas *property* rights are rights that protect

[58] Except of course the *legal* creation or recognition of the particular right in question.
[59] Penner at 112. This particular feature of property rights has been emphasised in scholarship considering whether property rights can subsist in a human body. Scholarship in this field brings into sharp relief the dichotomy that exists between property rights and personal rights. See in particular: Jesse Wall *Being and Owning* (Oxford University Press, Oxford, 2015) and Stephen Munzer *A Theory of Property* (Cambridge University Press, New York, 1990) at 37-56.
[60] Wall, above n 59, at 126.
[61] Penner at 111.

the choice to transfer.[62] In this way, the "right to transfer" has been said to be "an inherent feature of property rights."[63]

The concept of transferability underpins two frequently cited judicial articulations of the definition of property. It is the concept underlying Lord Wilberforce's statement in *National Province v Ainsworth*[64] that a property right: "must be … capable in its nature of assumption by third parties."[65] It is also the concept upon which Baroness Hale predicated the following definition of property:

> The essential feature of property is that it has an existence independent of a particular person: it can be bought and sold, given and received, bequeathed and inherited, pledged or seized to secure debts, acquired (in the olden days) by a husband on marrying its owner.[66]

Accordingly, it is clear that a right must be capable of transferability before it can be elevated to the category of property. As will be seen, however, the criterion of transferability poses a significant conceptual obstacle to the recognition of property rights in electronic data if the data is to be distinguished from pure information.

6. The rights are actionable per se

Another defining characteristic of property rights is that they are actionable *per se*. This means that property rights are not actionable upon proof of damage but are actionable upon mere interference with the right in question.[67] Property rights are actionable

---

[62] Munzer, above n 59, at 48-49.
[63] Penner, above n 56, at 80.
[64] *National Province v Ainsworth National Province v Ainsworth* [1965] UKHL 1, [1965] A.C. 1175.
[65] Ibid at 1247-8 per Lord Wilberforce.
[66] *OBG Ltd v Allan* [2007] UKHL 21, [2008] 1 AC 1 at 309 per Baroness Hale.
[67] See Wall, above n 59 at 147 and Sarah Green "Rights and Wrongs: An Introduction to the Wrongful Interference Actions" in D Nolan and A Robertson (eds) *Rights and Private Law* (Hart Publishing, Oxford 2012) at 538. To fully understand why property rights are actionable per se it is necessary to understand the relationship between rights and duties. A legal right always imposes a legal duty on some person or people. Property rights impose a duty of non-interference. This is because property law aims to give owners the right to exclusively determine the use of a thing. In other tortious contexts, such as negligence, the law is concerned with tangible harm to individuals. Accordingly, these harm-based torts impose a duty on citizens to take reasonable care not to harm other people. The corresponding right is therefore simply the right to have other people take reasonable care not to harm the right-holder. Proof of damage is therefore critical to the enforceability of the right. This is not the case with property rights.

without proof of damage to reflect the primary concern of property law, which is to protect the *relationship* between a rights-holder and a thing.[68] As noted above, a right is proprietary if it entitles the holder to *exclude* third parties from interfering with the right.[69] It follows, therefore, that any interference with a property right necessarily violates the right of exclusion and thus property rights do not require proof of damage to be actionable. It is not clear in New Zealand, however, whether *all* interferences with property rights are actionable without proof of damage.[70] Nevertheless, at a conceptual level of analysis, a property right protects an individual's exclusive relationship with a thing and thus proof of damage is unnecessary to establish a cause of action.

7. Conclusion

In sum, the term "property" refers to a set of rights that the law *chooses* to recognise as a means of protecting an individual's exclusive relationship with a particular thing. The following analysis considers whether, for the purposes of property law, the 'thingness' of computer data could lie in its physical existence rather than in the information it contains.

C The nature of computer data

The Court of Appeal in *Dixon* were alive to the possibility that a computer file could be distinguished from pure information on the basis that it is has a physical existence whereas pure information is an ideational entity. The Court acknowledged that:

> digital footage itself may be property while the information it contains is not. A digital file arguably does have a physical existence in a way that information (in non-physical form) does not.[71]

---

[68] Wall at 148.
[69] Worthington at 35.
[70] *Everitt v Martin* [1953] NZLR 298. See below n 183 for a fuller discussion on this point.
[71] At [30]. The Court also noted that there is a High Court decision holding that internet usage does qualify as "property" for the purposes of the Crimes Act: see *Davies v Police* CRI-2006-488-56, [2008] 1 NZLR 638 (HC). However, that case expressly distinguished internet usage from the information contained in the data, and did not consider the status of the latter. Accordingly, the facts in

As authority for this proposition, the Court cited the decision of *R v Cox* which held:

> Nor do we see anything in the argument that the electronic data is not "a thing". It has a physical existence even if ephemeral …"[72]

The Court in *Dixon*, however, decided that whatever the physical nature of a computer file, it is indistinguishable in principle from pure information because a computer file is "essentially just a stored sequence of bytes".[73] Whilst this is technically correct, the Court's conclusion requires a far more extensive discussion before it can be asserted that electronic data is indistinguishable in principle from pure information.

1. What is a computer file?[74]

As the Court states, a computer file is essentially just a stored sequence of bytes.[75] A "byte" is a unit of data that is eight binary digits long, (e.g. 10100110).[76] It is important to understand, however, that the reference to 1s and 0s is merely a representation of the two-state nature of the digital world.[77] The process of digitisation contrives two discrete states and these states are used to create a code that can be considered analogous to Morse code. In essence, this code is a set of *instructions* that causes a computer to organise and manipulate a screen's multitude of pixels to render information legible for a viewer.[78] In computer files, the two states used to create binary code have some physical realisation, such as positive and negative pulses of electrical voltage.[79] The storage hardware in the computer arranges physical media to

---

Dixon meant it was the first case requiring the courts to consider "property" in the context of electronically stored footage or images.

[72] *R v Cox* (2004) 21 CRNZ 1 CA at [49].

[73] At [31].

[74] I am indebted to David Eyers, Professor of Computer Science at Otago University, for his expertise and helpful comments regarding the technological aspects of a computer.

[75] B.S. Chalk, A.T. Carter and R.W. Hind *Computer Organisation and Architecture: An Introduction* (2nd ed.) (Palgrave Macmillan, Basingstoke, 2003) at 10.

[76] Ibid at 2: "The mighty computer can do little more than add two numbers together. Everything else we see the computer being used for, be it playing a graphics game, word processing a document or running a payroll is a sequence of operations that mainly involves adding numbers together."

[77] Ibid at 10.

[78] For a helpful summary on how a computer works see Martin Wasik *Crime and the Computer* (Oxford University Press, Oxford, 1991) at 5-6.

[79] I am grateful to David Eyers for his lucid explanation of this process.

represent the two states. This is sometimes achieved by the use of an electric current, to create either magnetised or unmagnetised space. The computer reads the patterns of magnetised and unmagnetised spaces with a read/write head as "on" and "off" or "0" and "1".[80] In this way, the machine-readable language or code is the physical manifestation of the information in binary form.[81] Accordingly, unlike pure information, digital data does have a realisation in the physical world. Evidence of this can be found in the fact that devices storing electronic data have a finite storage capacity or 'memory'. That is because there is finite physical space for the electronic data to occupy.[82]

The question becomes, therefore, whether the fact that a computer file has some physical realisation in the material world is sufficient to render it tangible property. The law of property is very comfortable with the idea of attaching property rights to physical objects. A physical object clearly satisfies the conceptual requirements of property as they have been outlined above. Admittedly, on the rare occasion, social and political considerations will preclude the admission of a physical object to the category of property.[83] However, the exclusion of a physical object from the aegis of property law should be seen as the exception that proves the rule. In other words, the case for computer data being property is significantly strengthened if it can be demonstrated that electronic data behaves like a physical object.

2. American authority

There is American authority to suggest that the physical existence of a computer file *is* sufficient to distinguish it from information and render it tangible property. The Louisiana Supreme Court, in the context of whether computer software is taxable tangible property, concluded that electronic data has a physical existence and is corporeal property.[84] The Court argued that an arrangement of matter, physically

[80] *South Central Bell Telephone Co. v. Sidney J. Barthelemy, et al*. 643 So.2d 1240 (1994), 1246.
[81] Ibid. See also Donald H. Sanders *Computers Today* (McGraw-Hill, 1988) at 229 and 233.
[82] David Berry *The Philosophy of Software* (Palgrave Macmillan, New York, 2011) at 98.
[83] For example, Canadian and U.S. legislators specified during the Prohibition era that no property rights were to exist in alcoholic beverages. The purpose of the legislation was to discourage commercial transactions in liquor. See above n 39.
[84] Above n 80.

recorded on some tangible medium, constitutes a corporeal body.[85] The Court summarised its arguments as follows:

> In sum, once the "information" or "knowledge" is transformed into physical existence and recorded in physical form, it is corporeal property. The physical recordation of this software is not an incorporeal right to be comprehended.[86]

Whilst this argument was made in the context of "computer software", which, as will be explained, is different from computer *data*,[87] the reasoning remains apposite to all electronic code. The Court considered the electromagnetic impulses comprising computer software to be corporeal property by virtue of their physical existence. The same reasoning is available in the context of a computer file, which is also comprised of electromagnetic impulses.

3. An incoherent physical existence

Taking a contrary position, Judge David Harvey,[88] writing extra-judicially, warns that despite the physical existence of a computer file, there is a "a danger in thinking of electronic data as an object 'somewhere there' on a computer in the same way as a hard copy book is in a library."[89] Judge Harvey argues that electronic storage media are constructed in such a way that it is "not possible for a complete file of electronic information to be stored in consecutive sectors in a medium."[90] Rather, the electronic information is distributed across a storage medium and are then "assembled, processed

---

[85] Ibid at 1246.

[86] Ibid at 1250. Note also that some American states have legislated to expand the definition of "property" for the purposes of theft, so as to include: "electronic impulses" and "electronically processed or produced data or information". See, for example, Mont Code Ann, s 45.2.101(54)(k) (1981). See also Wasik, above n 78, at 127. Note also that American courts have been less reluctant than commonwealth jurisdictions to recognise proprietary rights in confidential (pure) information. See, for example, *Carpenter v United States* 484 US 19 (1987); *People v Kwok* 63 Cal App (4th) 1236 (1998); and *People v Kozlowski* 96 Cal App (4th) 853 (2002). Recognising proprietary rights in electronic data is consistent with recognising proprietary rights in pure information.

[87] See below n 147. This distinction is discussed on page 34.

[88] Judge of the Auckland District Court.

[89] David Harvey "Digital Data and Theft – Collisions in the Digital Paradigm IV", July 29 2014 on "The IT Countrey Justice: An Occasional Blog about Law and IT": https://theitcountreyjustice.wordpress.com/2014/07/29/digital-data-and-theft-collisions-in-the-digital-paradigm-iv/.

[90] Ibid.

and rendered legible for a human user."[91] In the metaphorical digital "library" there do not exist discrete and complete data files as there are in the case of hardcopy books in a library. Instead, there is a seemingly random[92] and messy amalgam of electronic data as if all the books in a physical library were dissected into paragraphs and randomly distributed as scraps of paper throughout the bookshelves.

This analysis leads Judge Harvey to conclude that a computer file cannot be understood as a "single entity" as it does "not exist independently from the process that recreates it every time a user opens it on a screen."[93] Whilst, therefore, a computer file can be conceived of as a unique combination of electro-magnetic impulses, reified as an electronic matrix, the reality is that this electronic matrix does not exist as an independent entity. Instead, as in the case of a text file, there is "constant interactivity between the disk or medium interpreter, the code of the word processing program and the interpreter that is necessary to display the image on the screen."[94] The point here is that a computer file, irrespective of its physical existence often does not exist in a coherent and independent state.

Accordingly, the disparate existence of computer data makes it very difficult to conceive of a computer data as a physical *object*. The relevant question becomes, therefore, whether the disparate physical existence of a computer file provides a sufficient reason by itself to refuse to recognise the same structure of rights that the law normally recognises in tangible property.[95] It is certainly peculiar to recognise something as tangible property that has a disparate physical existence. This is evidenced by the sheer difficulty in imagining examples of tangible property items that exist in disparate form. The fact of rarity by itself, however, does not provide a convincing normative reason to change the structure of the rights subsisting in a computer file. In other words, the mere fact of incoherence is not a knockdown argument against recognising a computer file as tangible property. After all, the law of

[91] Ibid.
[92] The arrangement of electronic data would appear random to a human but not to a computer, which is a deterministic machine.
[93] Above n 89.
[94] Ibid; see also Burkhard Schafer and Stephen Mason "The Characteristics of Electronic Evidence in Digital Format" in Stephen Mason (ed) *Electronic Evidence* (3rd ed.) (LexisNexis Butterworths, London, 2012) at 2.06.
[95] For an elucidation on the structural features of property law see Wall, above n 59, at 141-174.

property is concerned only with the relationship between a person and some 'thing', whatever that particular thing may be.

Water is an example of a thing that is clearly not 'an object' that some jurisdictions have recognised as tangible property despite its disparate nature.[96] Those jurisdictions contend that the fluid, continuous nature of water does not provide a compelling normative argument against its recognition as tangible property. Accordingly, the disparate physical nature of electronically stored data must be fastened to normative argument before the refusal to recognise property rights in computer data becomes valid. Correspondingly, the fact that a computer file has some physical realisation must also be fastened to normative argument before that fact alone is sufficient to qualify computer data as property.

One possible argument is that computer data cannot exist in the material world without being housed in a storage medium of some kind. The comparison of digital data to traditional print media illustrates this point. Whereas traditional print media is seen in terms of the dichotomy that exists between the physical print medium and the intangible information it records, digital media can be described, for present purposes, as a trichotomy. There is (i) a computer, which provides the physical medium on which information can be viewed; (ii) electronic data, understood as a sequence of bytes; and (iii) the intangible information contained on the electronic data.[97] The question is whether the intermediary – a sequence of bytes – behaves more like tangible property or pure information. Admittedly, a sequence of bytes does play a similar role to physical print media in that it transforms "information or knowledge" into "physical existence and physical form".[98] Indeed, it is the tangibility of these binary digits that usefully allows intangible information to be digitally stored and transported. Thus, on

[96] I am grateful to Jesse Wall for suggesting this analogy. For a summary of the recognition of property rights in water in the United States of America see: Shelley Ross Saxer "The Fluid Nature of Property Rights in Water *21 Duke Environmental Law & Policy Forum* (Fall 2010) 49-112 at 54; see also *Hydro Res. Corp. v. Gray*, 173 P.3d 749, 757 (N.M. 2007): "the person who develops water by putting it to beneficial use becomes the owner of the water right and can put it to his own use, sell or lease it, or transfer it to a different place and purpose of use (subject to the requirement that it will not impair other rights)."

[97] Framing the issue in terms of a trichotomy ignores the role played by hardware and software in the expression of a computer file. However, hardware and software do not contain data; rather they are the tools that make data usable: see below n 147. Accordingly, hardware and software should be seen as being subsumed within the first prong of the trichotomy: the computer itself.

[98] Above n 80 at 1250.

this analysis, there are some similarities between electronic data and traditional print media.

Computer data, however, cannot be stored, transmitted or accessed without some storage medium[99] to contain it. Digital data cannot even exist independently of a medium. At this point, the analogy to traditional print media breaks down. Thus, there is a crucial difference between water and computer data because the former does not need a storage medium to exist in the material world. The fluid nature of water means it often requires a container, such as a drink bottle or a cistern, to be rendered as a useful resource but it does not require the container to *exist* in the first place. A droplet of rain exists is not *created by* a storage medium. On this analysis, electronic data is perhaps closer in kind to pure information than items of tangible property and therefore does not sit comfortably with the traditional conception of tangible property.

The foregoing argument, however, is unconvincing. It is entirely possible to draw a distinction between a storage medium and the binary digits it contains (and even creates). Computer data can still be a physical 'thing' regardless of whether its physical existence is ephemeral or even contingent on the role played by a particular storage medium. "Electricity", for example, is included in the criminal definition of "property".[100] Whether computer data qualifies as "electricity" is a separate issue discussed in the next chapter[101] but the point here is that Parliament has recognised electricity as a 'thing' in which property rights can inhere regardless of an ephemeral nature and dependence on an insulation medium. Accordingly, the lack of an independent physical existence should not be seen as sufficient by itself to countenance the exclusion of computer data from the category of tangible property. There is, however, a convincing conceptual objection to the recognition of property rights in the physical binary digits comprising a digital file: the impossibility of transfer.

[99] "Medium" in this sense means "a particular form of storage for digitised information". "Medium" was used earlier in respect of a computer screen to mean "a means by which something is communicated or expressed".
[100] Crimes Act, s 2.
[101] See discussion on pages 36-37.

4. The impossibility of transfer

The major conceptual obstacle to recognising property rights in the physical realisation of binary code lies in the impossibility of transfer. This is because the digital method of transmission means it is impossible to transfer rights in respect of the *same* physical binary digits.[102] Digital transmission involves duplicating the sequence of bytes that comprise electronic data, which means the recipient obtains a *copy* of the data. Correspondingly, the original possessor is not deprived of his or her data. Thus, if property rights were to subsist in a digital file, the original possessor could not transfer these rights in respect of the same digital file. Instead, what the recipient would receive would be identical rights in respect of an identical, *but different*, file. After transfer, both individuals would have relationships with identical but separate files. On this analysis, it is a logical impossibility to say there has been a *transfer* of rights in respect of the same physical thing. This is not a case of co-ownership, which the law of property recognises as a valid possibility,[103] because the alleged property rights in this case would operate in respect of different *physical things*.

The impossibility of transfer in the digital context brings into focus the distinction between "rivalrousness" and "excludability".[104] Rivalrous goods are goods, such as tennis rackets, where use by one consumer prevents simultaneous use by another.[105] On the other hand, a good is excludable simply when it is possible to prevent *some* people from using or enjoying it.[106] Accordingly, a concert performance is an excludable resource because concertgoers must pay for admission but the concert is non-rivalrous because multiple people can enjoy it simultaneously. Alleging the inherence of property rights in the *physical* code comprising a digital file reflects a desire to treat digital files as rivalrous goods. In other words, alleging the inherence of property rights in the *physical realisation* of computer data reflects a desire to protect

[102] It is of course possible to transfer the *same* binary digits by transferring the physical medium in which they are contained. That is not the type of transfer at issue.
[103] Above n 44.
[104] See Green, above n 23 at 208-209.
See also Lawrence B. Solum "Legal Theory Lexicon: Public and Private Goods," *Legal Theory Blog* (January 25, 2015), http://lsolum.typepad.com/legaltheory/2015/01/legal-theory-lexicon-public-and-private-goods.html.
[105] Above n 104.
[106] Ibid.

relationships with digital files with the same structure of rights that protects relationships with tennis rackets.

However, there is a fundamental difference between tennis rackets and digital files: it is possible to transfer the property rights inhering in *a particular* tennis racket but the nature of digital transmission renders it impossible to transfer any property rights inhering in a *particular* digital file. Accordingly, *if* the criterion of transferability is to be satisfied, a digital file must be seen as an excludable but non-rivalrous good. The excludability of a digital file rests in the right to decide whether or not to permit others to make a copy of the file. At this point, however, the physical realisation of a digital file becomes irrelevant to its excludability. Admittedly, as a matter of strict logic, this does not compel the equation of electronic data to pure information because electronic data is a set of instructions expressed as a two-character code, whereas pure information is what the code renders visible on a computer screen. However, at this level of abstraction, the distinction between them is – to trade on an ambiguity - "immaterial". This is because electronic data is simply the machine-readable version of the same information. Any distinction between the two would be unprincipled for the purposes of the law.

Property "protects the choice to transfer."[107] The only way property law can protect the choice to transfer computer data is if the data is conceived of at a higher level of abstraction than its physical existence. It is possible to satisfy the criterion of transferability in the context of digital transmission but only if the relevant relationship is seen as the relationship between an individual and the *information* expressed by a digital file. Thus, on the facts of *Dixon*, the relevant property rights could involve the right to exclusively control the CCTV *footage* rather than the right to use and control the particular digital *file* that held the footage.[108] On this view, the 'thing' is the footage (what a viewer sees through the organised manipulation of a screen's pixels) rather than the file itself. This shift in perspective, however, renders the relevant 'thing' as the information contained in a computer file rather than the physical file itself. Accordingly, at this level of abstraction, there is not a physical "thing" that property

[107] Above n 62.
[108] *Dixon* above n 1 at [20]: "what [the bar] lost was the right to exclusive possession and control of [the footage in its possession]."

rights can attach to. Rather, the relevant property right exists in respect to something intangible - the information itself. At this level of abstraction, the Court of Appeal is correct to hold that digital information cannot be meaningfully distinguished from pure information.

5. English authority

In addition, this conclusion is consistent with English authority. *Malone v Commissioner of Police*[109], which was a case involving telephone tapping, held that there could be no property (as distinct from copyright) in the electric impulses of a telephone system used to transmit the words of a conversation. The judge did not see any force in the argument that the physical realisation of information through electric impulses gave rise to property rights in those electric impulses. Given New Zealand is a common law jurisdiction, this English authority should carry more weight than the contrary decisions made in American jurisdictions.

D Conclusion

The fact of a computer file's physical existence is not sufficient to warrant it being classified as tangible property within the criminal definition of "property". Despite its physical existence, conceptual analysis instructs that computer data is rightly equated with pure information in the context of property. Accordingly, normative discussion regarding the admission of computer data to the category of property is properly conducted in respect of the information it contains. Thus, the decision to recognise rights that are both enforceable against an open-ended set of people and actionable without proof of damage turns on the desirability of recognising information as property. Nevertheless, Chapter IV reinforces the conclusion reached in this chapter with reference to the consequences that would accompany treating electronic data as property within the specific context of the Crimes Act.

[109] *Malone v Commissioner of Police*[109] (No 2) [1979] 2 All ER 624.

CHAPTER III

THE LEGISLATIVE HISTORY AND CONTEXT

A Overview

This chapter argues that an exercise in statutory interpretation also supports the equation of electronic data with pure information and the wider proposition that the definition of "property" in the Crimes Act does not extend to electronic data. The chapter surveys the relevant legislative context and history in order to ascertain whether Parliament intended for the Crimes Act's definition of "property" to extend to a computer file. It is concluded that the relevant legislative history and context militate against including electronic data in the criminal definition of "property". Finally, this chapter considers whether the electronic nature of computer data is sufficient to qualify it as property by virtue of the reference to "electricity" in the s 2 definition of "property". This argument is rejected.

B The legislative history

In 2003, Parliament introduced a raft of amendments to the Crimes Act in an attempt to modernise the criminal law, specifically in the context of computer crime.[110] The definition of "property" in s 2 was updated and a number of provisions were added to Part 10 of the Act under the heading "crimes involving computers". The relevant question is whether these changes evince Parliament's intention to include electronic data within the criminal definition of property.

Legislative amendment was catalysed by the case of *Wilkinson*,[111] which clearly demonstrated that advances in electronic and information technology had "outflanked

[110] These changes were implemented by the Crimes Amendment Act 2003, which came into force on 1 October 2003.

[111] *R v Wilkinson* [1999] 1 NZLR 403 (CA). The issue was whether electronic money being transferred across bank accounts was the "property of any person" and whether it was "movable". On whether the money was the "property of any person", the majority observed that no money actually moves through the modern banking system. Instead there is a debiting of one bank account and a corresponding crediting of another bank account. When Wilkinson's bank account was credited, he did not obtain the lending

the explicit wording" of some criminal provisions.[112] Before legislative amendment, s 217 of the Crimes Act required property to be movable before it could be stolen.[113] It was therefore irrelevant that the definition of "property" in s 2 included choses in action[114] because the provisions relating to the unlawful obtainment of property were only activated if the property in question was movable. After reluctantly quashing the relevant convictions, the Court appealed to Parliament for remedial legislation,[115] which came in the form of the Crimes Amendment Act 2003.

In the course of drafting the amendment, the Law and Order Select Committee suggested having a definition of "property" specifically for Part 10 of the Crimes Act. The proposed s 305A that would have been inserted by cl 19 of the Crimes Amendment Bill (No 6) 1999 (322-1) provided the following definition of "property":

> Property includes real and personal property, and all things, animate or inanimate, in which any person has any interest or over which any person has any claim; and also includes money, things in action, and electricity.[116]

The Court of Appeal in *Watchorn*[117] considered this definition to be "broad enough to include computer data."[118] Although the Court did not explain how it reached this conclusion, it likely reasoned along the following lines. The proposed definition renders as property "all things … in which any person has any claim" and thus computer

institution's chose in action. On the contrary, that chose in action was extinguished and a new equivalent chose in action was brought into existence. In this way, the appellant did not take the "property of any person." The Court then went on to hold that a chose in action was not movable as envisaged by s 217 thus a charge of theft was not possible anyway.

[112] Ibid at 412 per Thomas J.

[113] Crimes Act, s 217: the only things "capable of being stolen" were "every inanimate thing whatsoever, and every thing growing out of the earth, which is the property of any person, and either is or may be made movable, is capable of being stolen as soon as it becomes movable, although it is made movable in order to steal it."

[114] The pre-2003 definition of "property" was exactly the same as it is now except for the latter's specific references to "money" and "electricity".

[115] *Wilkinson*, above n 111 at 412-14 per Thomas J.

[116] Crimes Amendment Bill (No 6) 1999 (322-1); Law and Order Committee Crimes Amendment Bill (No 6) and Supplementary Order Paper No 85 (20 July 2001) at 17.

[117] *Watchorn v R* [2014] NZCA 493 at [75]. The issue in *Watchorn* was whether downloading digital files containing sensitive commercial information qualified as "obtaining property" under s 249. The Court considered itself to be bound by the decision in *Dixon* and so answered the question in the negative without engaging with the argument. Instead, the issue was whether Mr Watchorn had obtained a "benefit".

[118] Ibid at [75].

data qualifies as property because it is a thing in which a person has a claim to possession.

In the end, however, Parliament discarded the proposed s 305A and simply amended the definition of "property" in s 2 to include "money" and "electricity". It can be inferred from the decision to enact the narrower of the two proposed definitions that the current definition of "property" does not extend to electronic data. As the Court in *Dixon* put it:

> The amendment [to the definition of "property"] was limited. It consisted only of the addition of money and electricity. Parliament must be taken to be aware of the large body of authority regarding the status of information and in our view had it intended to change the legal position, it would have expressly said so by including a specific reference to computer-stored data. [119]

This conclusion can be reinforced with reference to the 1999 Computer Misuse Report. [120] That report expressly refers to the possibility of the "redefinition of information as a property right". [121] The fact that the Law Commission considered redefining information as a property right in the context of computer misuse suggests that Parliament considered electronic data to be equivalent to pure information. [122] If a computer file were deemed to be an item of property as separate from the information it contains then it would be unusual for the Law Commission to be considering information as a property right in the context of computer misuse. As there is no reference to information as a property right in the Crimes Act, Parliament should be taken to have decided against the redefinition of information as property. [123] This further supports the conclusion that electronic data is not currently "property" for the purposes of the Crimes Act.

[119] *Dixon* above n 1 at [35].
[120] Law Commission Computer Misuse (NZLC R54, 1999).
[121] Ibid at [36].
[122] *Dixon* above n 1 at footnote 20.
[123] Ibid at [35].

C The legislative context: the Crimes Act

1. Section 249

It is necessary to contextualise the question of whether a computer file is "property" for the purposes of the Crimes Act by having regard to the relevant provisions of the Act itself. A useful starting point is the section Mr Dixon was charged under: s 249. Section 249 of the Crimes Act criminalises the obtaining of "property" through the dishonest access of a computer system. The Court in *Dixon* considered whether Parliament, by creating a crime of accessing a computer in order to obtain property, must have intended electronic data to be "property".[124] The argument is that Parliament's reference to "property" in this provision would be otiose if electronic data were not to qualify as "property". The Court of Appeal rejected this argument and considered the offence to be aimed at situations where a defendant accesses a computer and uses, for example, credit card details to unlawfully obtain goods.[125] Giving credence to this argument is the inadequacy of s 240 - "obtaining [property] by deception" - in the context of a computer.[126] The authors of *Adams on Criminal Law*[127] have argued that the requirement that deception be an operative cause of the obtaining under s 240 excludes the obtainment of goods or money from an automated machine.[128] As King CJ held in the Australian case *Kennison v Daire*[129] a machine "cannot be deceived by a false pretence or other fraud."[130] A computer is an automated machine because it simply executes the list of instructions it is fed. On this analysis, s 240 would be ineffective in criminalising the fraudulent use of a computer to obtain property. The reference to "property" in s 249, therefore, is a necessary inclusion in the Crimes Act irrespective of whether electronic data qualifies as property.

---

[124] Ibid at [38].
[125] Ibid at [38].
[126] Crimes Act, s 240: "Every one is guilty of obtaining by deception or causing loss by deception who, by any deception and without claim of right obtains ownership or possession of, or control over, any property. In this section, deception means a false representation, whether oral, documentary, or by conduct, where the person making the representation intends to deceive any other person."
[127] Bruce Robertson and Jeremy Finn *Adams on Criminal Law 2014* (Student ed) (Thomson Reuters, Wellington, 2014) at 391.
[128] Ibid.
[129] *Kennison v Daire* (1985) 38 SASR 404, 16 A Crim R 338 (affirmed *Kennison v Daire* (1986) 160 CLR 129, 60 ALJR 249).
[130] Ibid at 406. See also above n 120 at [64].

In addition to obtaining "property", s 249 criminalises the dishonest obtainment of any "privilege, service, pecuniary advantage, benefit, or valuable consideration". How "benefit" and "privilege" are construed is therefore critical to the present discussion because the scope of these terms will largely dictate the scope of the computer activity criminalised by s 249 if electronic data does not qualify as property. The Court in *Dixon* interpreted "benefit" broadly to include the "opportunity to sell the footage".[131] The Court then noted that their conclusion that electronic data is not property "does not in any way frustrate Parliament's decision to criminalise the misuse of computers" because the term "benefit" was sufficiently broad to sustain Dixon's conviction.[132] Thus, Dixon was ultimately convicted for "obtaining a benefit" rather than "obtaining property". It is necessary, however, to determine whether the Court's broad construction of "benefit" is warranted by the statutory context or whether it subverted Parliament's intention.

The scope of the phrase: "privilege, service, pecuniary advantage, benefit, or valuable consideration" was considered at length in *Watchorn.*[133] The Court concluded that there was not "any proper basis to limit the scope of the term "benefit" to financial advantage or to limit its normal meaning of anything that is of advantage to the person concerned".[134] The Court endorsed the decision in *Police v Le Roy*[135] that "privilege" or "benefit" in the section can extend to non-monetary advantages. *Le Roy* considered that a non-monetary advantage might be:

> the acquiring of knowledge or information to which one was not otherwise entitled. The advantage might be the invasion of another's privacy. It might be knowledge or information that could be used to exploit another person.[136]

Further support for a wide interpretation of "benefit" can be found by contrasting s 249 with s 228. Section 228 makes it an offence to obtain any document dishonestly and without claim of right with intent to obtain any "property, service, pecuniary advantage

[131] *Dixon* above n 1 at [39].
[132] Ibid.
[133] *Watchorn*, above n 117, at [68]-[81].
[134] Ibid at [81].
[135] *Police v Le Roy* HC Wellington CRI-2006-485-58, 12 October 2006.
[136] Ibid at [11].

or valuable consideration". The terms "benefit" and "privilege" are conspicuously absent. As the Court in *Watchorn* notes,[137] their omission from s 228 was a result of the Select Committee's decision that those terms should be omitted to make it clear that s 228 related only to financial benefit.[138] The inclusion of these terms in s 249 suggests by implication, therefore, that the section has a wider ambit than merely "property" and financial benefits. As a result, the Court in *Watchorn* suggested as *obiter* that "possession and control of, and therefore opportunity to use … downloaded files" *could* constitute a "benefit" for the purposes of s 249(1)(a).[139] The statutory context and consistency of precedent suggest this is the correct legal approach. This approach accords with Parliament's purpose of criminalising computer misuse and with the contention that digital information is not property.

2. Other crimes involving computers

The other provisions dealing with computer misuse also provide relevant context. In 2003, Parliament introduced a host of provisions specifically targeting computer crime.[140] These provisions were drafted widely in an attempt to prevent them being rendered anachronistic by further technological advancement. The key point for present purposes is that the computer crime provisions focus on the defendant's *mens rea* – or guilty mind - rather than any specific methods for the commission of a computer crime. The sections criminalise "accessing [a] computer system[141] for [a] dishonest purpose",[142] "damaging or interfering with [a] computer system",[143] "making, selling or distributing or possessing software for committing crime",[144] and

[137] *Watchorn* above n 117 at [76].
[138] Above n 116.
[139] *Dixon* above n 1 at [83] (emphasis added).
[140] Sections 248-254 were introduced under the heading "Crimes involving computers". Sections 253 and 254, which gave the Security Intelligence Service and GCSB qualified exemption access to computers without authorisation, have since been repealed.
[141] Crimes Act, s 248(a)(i) defines a "computer system" in terms of a "computer," which is not further defined. The word "computer" has come in common parlance to refer to electronic machines operating as digital computers: *Adams on Criminal Law* at 403. *Pacific Software Technology v Perry Group Ltd* (2003) 7 NZBLC 103,950 (CA), at 103,953 considered a digital computer to constitute "five functional elements: (i) input; (ii) storage of that input by a memory system; (iii) a control unit which receives data from memory and gives instructions for the necessary arithmetic; (iv) an arithmetic which carries out the control commands; (v) an output capacity."
[142] Crimes Act, s 249.
[143] Crimes Act, s 250.
[144] Crimes Act, s 251.

"accessing [a] computer system without authorisation".[145] As can be seen, the operative verbs have an intentionally broad gamut in order to avoid references to technological specifics, which could provide relief to calculated miscreants in the form of technicalities. Consequently, the focus on *criminal intention* rather than specific technological activities, coupled with the breadth of the term "benefit" in s 249, means the efficacy of the computer crime provisions does not turn on the definition of "property".

Moreover, the definition of "access" in relation to a "computer system" strongly suggests that Parliament did not intend for digital data to qualify as "property". The term "access" in relation to a computer system means: "instruct, communicate with, store data in, receive data from, or otherwise make use of any of the resources of the computer system."[146] The inclusion of the phrase "receive data from" in the definition of "access" makes it problematic to treat computer data as property in the context of computer crime. To illustrate this point, s 249 can be read after substituting the term "access" with the phrase "receive data from" (taken from its definition) and the term "property" with the term "data". Section 249 would then read: "everyone is liable to imprisonment who, directly, or indirectly receives data from any computer system and thereby obtains any data." These substitutions render the provision a nonsensical tautology. Further, the definition of "computer system" in s 248 includes "stored data". This suggests that Parliament did not intend for computer data to be an entity separate from the computer on which it is stored. Accordingly, the definitions of "access" and "computer system" in s 248 provide further contextual support for the contention that the criminal definition of property does not extend to computer-held data.

3. Sections 217 and 230

The way s 230 operates in conjunction with the definition of "document" in s 217 also supports the equation of computer data to pure information. Section 230 criminalises the copying or taking of "documents" containing "trade secrets". As the Court notes in *Dixon*, this provision would serve no practical purpose if confidential information were

[145] Crimes Act, s 252.
[146] Crimes Act, s 248.

treated as property because other property-related provisions would criminalise the unlawful appropriation of confidential information.[147] More relevant to the present question, s 230, through the definition of "document" in s 217, seems to target the unauthorised obtainment of *digitised* trade secrets. This is because the definition of "document" was modernised in 2003 to include:

> …
>
> (c) any disc, tape, wire, sound track, card, or other material or device in or on which information, sounds, or other data are recorded […] so as to be capable, with or without the aid of some other equipment, of being reproduced; or
> (d) any material by means of which information is supplied […] to any device used for recording or storing or processing information; or
> (e) any material derived […] from information recorded or stored or processed by any device used for recording or storing or processing information.[148]

As can be seen, this provision goes to great lengths to include any medium on which electronic data can be stored without ever treating electronic data *as a "document"*. The effect of this is that the medium-message dichotomy[149] that applies to paper documents also applies to computer files. In criminalising the copying of a trade secret in digital form, s 230 targets the mediums on which digitised trade secrets can be stored as opposed to the digitised trade secret itself. This further suggests that Parliament considered the status of electronic data to be equivalent to that of pure information in the context of the Crimes Act.

4. Conclusion

The above provisions lend contextual support to the argument that electronic data is not "property" for the purposes of the Crimes Act. However, given the incorporative nature of the definition in s 2, it is necessary to survey other New Zealand statutes that define "property".

---

[147] *Dixon* above n 1 at [37].
[148] Crimes Act, s 217.
[149] This dichotomy refers to pure information as the "message" and the instrument on which it is stored as the "medium".

D The legislative context: other statutes defining "property"

There are a number of other New Zealand statutes with definitions of "property". On the basis that the Crimes Act imports conceptions of property from the general law these statutes can be used to inform the Crimes Act's definition of "property". These are considered in turn.

1. Property (Relationships) Act 1976

The Property (Relationships) Act 1976 defines "property" in almost the identical terms used in the criminal definition.[150] The definition of "property" in s 2 of the Property (Relationships) Act defines "property" to include:

> (a) real property:
> (b) personal property:
> (c) any estate or interest in any real property or personal property:
> (d) any debt or any thing in action:
> (e) any other right or interest.

The purpose of the Property (Relationships) Act is to divide the relationship property of couples after separation or death.[151] Accordingly, the Act requires a wide definition of property if it is to achieve an effective division of relationship property. The fact that the criminal definition is drafted in almost identical terms could perhaps suggest it has a correspondingly wide scope but it does not throw any light on the specific question of whether electronic data qualifies as property.

2. Statutes pertaining to consumer issues

In 2003, however, a raft of statutes pertaining to consumer issues were amended to include updated definitions of "goods" that now refer to "computer software". The

[150] The only difference is the exclusion of specific references to "money" and "electricity" in the definition of "property" in the Property (Relationships) Act 1976.
[151] Property (Relationships) Act 1976, s 1C: "This Act is mainly about how the property of married couples and civil union couples who have lived in a de facto relationship is to be divided up when they separate or one of them dies. The Act provides that "in general, the couple's property is to be divided equally between the couple."

Sale of Goods Act 1908,[152] Fair Trading Act 1986,[153] Commerce Act 1986[154] and the Consumer Guarantees Act 1993[155] all define "goods" (which are necessarily items of "personal property") to include "computer software". These statutes define "goods" in the following way:

> "**goods**" means personal property of every kind (whether tangible or intangible); and includes […] to avoid doubt computer software."[156]

The use of the phrase "to avoid doubt" is interesting in that it suggests computer software already fits within the definition of "personal property" and does not require its own specific subsection to qualify as property. The critical question becomes, therefore, whether "computer software" includes the data comprising a digital file. Commentary in *Gault on Commercial Law* suggests that it does not:

> Although the Act defines computer software as being goods, there is an important distinction between software and data. The materials downloaded are data; the software is what is used as the tools to effect the download and make the data usable.[157]

The distinction makes sense in that computer software forms part of the machinery required for the operation of a computer whereas computer data is merely information in electronic form. Even though both computer software and computer files are composed of bytes, software makes a computer work in a particular way; it is what acts on and organises the bytes that comprise a computer file. It becomes part of the computer's processing machinery and can be seen therefore an extension of the computer itself, distinct from the data it operates on.[158] On this analysis, computer data should not be considered "property" by virtue of the reference to "computer software" in the aforementioned consumer statutes.

---

[152] Sale of Goods Act 1908, s 2.
[153] Fair Trading Act 1986, s 2.
[154] Commerce Act 1986, s 2.
[155] Consumer Guarantees Act 1993, s 2.
[156] See above n 152- 155.
[157] Barry Allan and Thomas Gault *Gault on Commercial Law* (Thomas Reuters, Wellington, 2010) 3-30; 3A.2.03.
[158] Glazebrook J made this point in the course of oral argument in *Dixon v R*, above n 6, at 30.

3. Property Law Act 2007

Finally, the Property Law Act 2007 provides a relatively recent statutory definition of "property". This Act should be seen as a valuable contextual resource because of its general purpose:

> the purpose of [the Property Laws Act] is to restate, reform and codify (in part) certain aspects of the law relating to real and personal property.[159]

On the basis that the Crimes Act's definition of "property" imports its conceptions of property from the general law, an Act with this purpose should be informative. For the purposes of the Property Law Act, "property":

> (a) means everything that is capable of being owned, whether it is real or personal property, and whether it is tangible or intangible property; and
> (b) includes any estate or interest in property.[160]

Defining property in terms of ownership marks a departure from previous statutory definitions of property. The definition in the Property Laws Act could reflect the argument that property is simply shorthand for anything that is capable of being owned.[161] On this footing, David Boldt, arguing on behalf of the Crown in the Supreme Court, tendered the following submission:

> Plainly a digital file is capable of being owned and it is owned. If any of us drafts a document on our computer or takes a digital photograph, it's ours, every bit as much as the hardware on which it's created and we are entitled to do with it as we pleased [sic], as long as we act lawfully.[162]

---

[159] Property Laws Act 2007, s 3.
[160] The Act also defines "property" to include the proceeds of any property in the context of the provisions which deal with the "setting aside of dispositions that prejudice creditors: s 345(2).
[161] This appears to have been the approach taken by the English and Welsh Court of Appeal in *Yearworth v North Bristol NHS Trust* [2009] EWCA Civ 37, [2009] 2 All ER 986 (CA). The issue was whether frozen sperm was the property of the sperm donors. The Court analysed ownership in terms of the degree of control sperm donors had over their frozen sperm. The Court considered the right to destroy the sperm as indicative of ownership and therefore held that the frozen sperm were the property of the donors.
[162] *Dixon v R*, above n 6, at 29.

In response, it is argued that framing the issue in terms of ownership does not change its substance in any way. The concept of ownership is merely a convenient reference to an individual's possession of certain property rights.[163] Accordingly, framing the issue in terms of ownership simply approaches the same coin from its other side. Thus, Boldt's submission does not obviate the need to consider whether property rights subsist in a computer file in the first place, which is the very point of this dissertation. Apart from referring to the concept of ownership, the definition of "property" in the Property Laws Act does not differ in substance from its criminal equivalent. Accordingly, the definition of property in the Property Laws Act 2007 does not add any contextual support for the inclusion of computer-held data in the criminal definition of property.

4. Conclusion

A survey of the various New Zealand statutes merely reinforces that it is not possible to exhaustively define property. The reference to "computer software" in the definitional sections of consumer statutes could possibly be seen as including electronic data within the ambit of property but the distinction between software and data suggests the contrary. Accordingly, these definitions do not cut against the earlier conclusion that Parliament intended to exclude computer data from the criminal definition of "property".

E Electricity?

The 2003 amendment to the criminal definition of property included the addition of "electricity". As explained, computer files are often composed of a series of electromagnetic impulses. It is possible, therefore, that the electronic nature of computer data could render it "electricity" and therefore "property". The following analysis argues against this possibility.

[163] As Bruce Ackerman puts it: "whenever a judge says Jones rather than Smith is 'the' property owner, he should be understood to mean: 'in one or another resource conflict between Jones and Smith, the legal system places an entitlement in Jones's bundle of rights rather than Smith's bundle.'" See Ackerman, above n 15, at 27.

1. Incoherence

David Harvey has contended that the inclusion of "electricity" in the criminal definition of "property" cannot apply to data in the digital space because of the "incoherence of the data".[164] Judge Harvey is advancing the same argument as he did in respect of whether digital data can be considered a single entity. His argument postulates that an incoherent existence necessarily disqualifies a computer file from the category of tangible property. As argued above, it is submitted that the proper approach is to connect the fact of incoherence to a normative argument. Electric currents have an inherently disparate existence[165] and yet the criminal definition of property still recognises the inherence of property rights in "electricity". Accordingly, Judge Harvey's objection is not the complete answer, as it fails to attach the fact of incoherence to a normative argument. The following analysis suggests an alternative argument.

2. Statutory purpose

The inclusion of "electricity" in the criminal definition of property accompanied the simultaneous repeal of (the then) s 218 of the Crimes Act, which criminalised the "abstraction of electricity".[166] Accordingly, the addition of "electricity" to the definition of property represents a conceptual shift in the criminalisation of unlawful abstraction of electricity. Presumably, Parliament decided that abstraction of electricity was appropriately governed by the laws of theft and did not require its own provision.[167] However, the addition of "electricity" to the criminal definition of "property" is directed at the same wrong: the misappropriation of electricity from its suppliers. Accordingly, the argument is not that the electricity comprising a computer file lacks an independent existence but that the electricity itself is not the valuable resource requiring the

[164] See above n 89 and discussion on pages 18-19.
[165] Electricity is just a flow of electrons and does not share, therefore, the attributes of a physical object.
[166] Crimes Amendment Act 2003, s 15.
[167] As Stuart Green has observed, electricity can be "stolen" in at least two ways. Consumers can tamper with the meters in their houses so as to be billed at a rate lower than their actual usage or they can tap into the wire between the electrical substation and their homes, thereby bypassing the meter entirely. In both cases the offenders are receiving electricity they have not paid for. See Green, above n 20, at 226-227. In England, "abstraction of electricity" is still its own provision and "electricity" does not fit within the Theft Act's definition of "property". See Theft Act (UK) 1986, s 13 and *Low v Blease* (1975) 119 Sol J 695; [1975] Crim LR 513.

protection of the property law. The "electricity" referred to in the criminal definition of "property" is a source of energy whereas the electricity comprising a computer file is merely the mechanism by which a computer screen is able to project information. Consequently, there are very different normative grounds for recognising property rights in the electricity supplied by power companies and the electricity comprising a computer file.

F Conclusion

The foregoing analysis suggests that Parliament intended for computer data to be equated with pure information in the context of the Crimes Act. Accordingly, the legislative history and context militate against the inclusion of computer data in the criminal definition of "property". Similarly, a review of the legislative history and context suggests that computer data does not qualify as "electricity" within this definition. The next chapter buttresses this conclusion with reference to the legal consequences that ensue if computer data is excluded from the definition of "property" found in the Crimes Act.

CHAPTER IV

THE LEGAL CONSEQUENCES

A Overview

This chapter examines the consequences of excluding computer data from the criminal definition of "property". This chapter first considers whether the private law affords individuals, whether expressly or obliquely, a legal right to the exclusive use of a digital file. If the private law does afford these rights then the inclusion of electronic data into the criminal definition of "property" may be undesirable. The next step is to articulate the legitimate grounds for criminalising unauthorised digital transfers in order to assess when criminal sanctions should accompany any protection granted by the private law. Finally, this chapter examines the property-related provisions of the Crimes Act in order to see whether the exclusion of electronic data from the criminal definition of property results in any inconsistencies or absurdities. It is ultimately concluded that the exclusion of electronic data from the definition of "property" best serves the objectives of the criminal law.

B The private law

It is argued below that the private law protects an individual's right to the exclusive use of a computer file through two distinct legal avenues. First, the law of intellectual property gives authors[168] the exclusive right to control the distribution of any digitised copies of their work. Secondly, traditional property law offences afford protection to the possessor of a computer file because computer data is necessarily stored in a

[168] Copyright Act 1994, s 5: (1) For the purposes of this Act, the **author** of a work is the person who creates it. (2) For the purposes of subsection (1), the person who **creates** a work shall be taken to be,— (a) in the case of a literary, dramatic, musical, or artistic work that is computer-generated, the person by whom the arrangements necessary for the creation of the work are undertaken: (b) in the case of a sound recording or film, the person by whom the arrangements necessary for the making of the recording or film are undertaken: (c) in the case of a communication work, the person who makes the communication work: (d) in the case of a typographical arrangement of a published edition, the publisher.

physical medium of some kind that will attract proprietary protection. These two legal avenues are considered in turn.

1. Copyright

Copyright is a property right.[169] It is the exclusive right to "copy a work" and to "issue copies of a work to the public, whether by sale or otherwise".[170] In other words, copyright gives the right-holder the *exclusive* right to control the distribution of a work. This is how the law reconciles the interests of a creator of a work and the interests of the multiple owners possessing copies of the work created by duplicative processes.[171] Rights of title and copyright exist concurrently. That is the elegant method by which the law is able to protect physical possession of an object while simultaneously protecting both artistic integrity and the right to profit from labour. Copyright, therefore, affords an author an exclusive right to control the distribution of the file. Moreover, copyright inheres in any computer file that is subsequently transmitted to a third party, which means the author of a computer file will have a remedy against an unauthorised recipient of the file because digital transmission necessarily involves 'copying'. Thus, subject to a number of exceptions,[172] copyright affords the authors of computer files the exclusive right to copy and distribute a computer file.

The pertinent question then becomes when copyright will inhere in a computer file. Leaving the requirement of "originality" aside, the Copyright Act has been drafted to ensure copyright protection can extend to any digitised version of a work. A computer file containing any text is capable of qualifying as a "literary work,"[173] which is defined to include "any work … that is written".[174] A digital photograph is capable of qualifying because "artistic work"[175] is defined to include "a photograph regardless of

[169] Copyright Act 1994, s 14. Rather than being one property right, "copyright" actually comprises a bundle of rights. For a list of these rights see Copyright Act 1994, s 16(1).
[170] Ibid.
[171] Green, above n 23, at 206: "Intellectual property law is designed to balance the economic interests of creators in reaping the rewards of their efforts against those of society in having access to a free flow of new ideas."
[172] See Part 3 of the Copyright Act 1994 which details a number of acts permitted in relation to copyright works.
[173] Ibid, s 14.
[174] Ibid, s 2.
[175] Ibid, s 14.

artistic quality".[176] Similarly, a digital sound file could qualify as a "sound recording"[177] and a digital file containing a film could qualify as a "film", which is further defined to mean "a recording on any medium from which a moving image may by any means be produced."[178]

Once something does qualify for copyright protection, then every unauthorised digital transmission would amount to an infringement of copyright. That is because the transmission of a digital file involves its precise duplication and thus, transmission necessarily infringes copyright by copying.[179] Secondly, if copyright does not subsist in a computer file due to the absence of sufficient originality[180] then the law legitimately refuses to acknowledge property rights in the information itself. This is because the information-gatherer has not exercised a sufficient degree of labour or creative spark to warrant the protection of copyright. Instead, the law protects the exclusive use of the information by protecting the rights inhering in the storage medium on which the data is contained.

2. Property rights in storage mediums

Digital data requires a storage medium.[181] Storage mediums are items of personal property. Accessing a storage medium without authorisation for the purpose of obtaining a digital file, therefore, necessarily constitutes an interference with the property rights subsisting in the storage medium itself. The correlation of a property right is a duty of non-interference[182] and thus any unjustified interference with the plaintiff's possession constitutes the tort of trespass provided the interference is direct and immediate.[183] Gaining possession of a storage medium for the purpose of obtaining

[176] Ibid, s 2.
[177] Ibid, s 14.
[178] Ibid, s 2.
[179] Ibid, s 30.
[180] It is unclear in New Zealand whether copyright would subsist in the electronically stored footage of Mr Tindall recorded by the Queenstown bar's CCTV camera. This is because there may not be a sufficient degree of originality in security footage to qualify for copyright protection. See Susy Frankel *Intellectual Property in New Zealand* (2nd ed) (LexisNexis, Wellington, 2011) at 246.
[181] A computer or a portable medium such as a USB stick or a hard drive.
[182] Above n 67.
[183] Todd, above n 51, at 543-544: "Trespass requires direct physical interference with goods. It can be to take goods away even though no material damage results to them or to use goods without authority." There is, however, authority in New Zealand holding that there is no right of action in the case of merely accidental contacts where no damage is done and that a plaintiff is not liable, even for nominal damages,

data clearly qualifies as a deliberate and direct interference with that storage medium. Further, the act of obtaining data from a storage medium necessarily involves asportation and therefore dispossession of the owner's storage medium, which has been held to be actionable *per se*.[184] Thus, it is likely a victim of the unauthorised abstraction of data from a storage medium would have an actionable claim for trespass to goods.

The appropriate remedy, however, is not always clear. The problem in the present context is that gaining temporary possession of a storage medium does not damage the medium itself and the act of transferring data does not actually damage or remove the original data contained in that medium. However, at least in theory, the courts can use vindicatory damages to compensate the violation of property rights where no physical property damage ensues.[185] In the context of trespass to land, a disturbance of privacy may be factored into the assessment of damages.[186] Thus, in *Ramsay v Cooke*[187] where there had been repeated and deliberate crossing of the plaintiff's land by the defendants in an arrogant manner, the plaintiffs were awarded aggravated damages of $2,500. Holland J held that the plaintiffs were "clearly entitled to damages because of their loss of privacy and their rights as landowners to keep others off."[188] The judge in this case used aggravated damages to attach practical significance to the duty of non-interference that follows from the existence of property rights. Similarly, trespass to goods is sometimes used to protect privacy.[189] It is possible, therefore, that unauthorised abstractions of computer data would be factored into an assessment of damages resulting from a claim of trespass to goods.

The English case *Thurston v Charles*[190] is instructive on this point. In that case, the defendant wrongly communicated to another person the contents of a letter written by

---

on account of casual and unintended contact with a defendant's property. See *Everitt v Martin*, 303 (endorsed in *Wilson v Marshall* [1982] TasR 298). That case, however, did not decide whether damage is required for the tort to crystallise in the context of intentional contacts. Accordingly, the case is not authority for the proposition that damage is required for the tort to crystallise in the context of intentional interferences with property.

[184] See Christian Witting and John Murphy *Street on Torts* (13th ed) (Oxford University Printing Press, Oxford, 2012) at 304. The act of deliberate asportation puts unauthorised abstractions of computer data outside the scope of the ratio in *Everitt v Martin*.

[185] Ibid. See also Todd above n 51 at 848.

[186] Todd, above n 51.

[187] *Ramsay v Cooke* [1984] 2 NZLR 680.

[188] Ibid at 687.

[189] Above n 51.

[190] *Thurston v Charles* 1905 21 TLR 659.

a third party to the plaintiff. The plaintiff brought an action to recover damages for the detention and conversion of the letter.[191] It was held that the plaintiff could recover substantial damages and not merely the value of the thing converted. Walton J held that the "kind the property in a thing like a letter is mainly valuable because it gives the plaintiff the right to keep it private."[192] The judge then held that "if a letter like this is taken and read and shown, it is a case where the plaintiff has a right to recover substantial damages."[193] Damages of £400 were awarded along with costs, which, in 1905, was a considerable sum of money. Accordingly, *Thurston v Charles* has been considered authority for the proposition that consequential damages flowing on from an interference with property are available.[194]

3. Conclusion

The foregoing analysis suggests that the law of property, through the tort of trespass to goods and through the law of copyright, affords possessors of digital files a legal right to exclusively control their electronic data. The next step is to articulate when the unlawful abstraction of this data also warrants criminal liability.

C The appropriate grounds for criminalisation

In general terms, the central idea of a crime is that it is something that appropriately concerns the State, and not just the parties affected by the wrongdoing.[195] As Andrew Ashworth notes:

> Many crimes are civil wrongs as well, and it is for the injured party to decide whether or not to sue for damages. But the decision to make conduct into a crime implies there is a public interest in ensuring that such conduct does not happen and that, when it does, there is the possibility of State punishment.[196]

---

[191] Ibid at 659.
[192] Ibid at 660.
[193] Ibid.
[194] See Witting and Murphy, above n 182, at 687.
[195] Andrew Ashworth *Principles of Criminal Law* (7th ed) (Oxford University Press, Oxford, 2013) at 2.
[196] Ibid.

Thus, it is necessary to identify when it is appropriate for the State to impose criminal sanctions that run parallel with the rights and remedies afforded to individuals by virtue of the private law. The following discussion seeks to articulate the appropriate grounds for criminalisation by identifying the various computer-related wrongs that warrant criminal sanctions. It is illuminating to first consider the rationale underlying intellectual property because that is the branch of the law specifically concerned with the unauthorised copying of information. Subsequently, it needs to be determined what types of copying deserve the imposition of criminal sanctions in addition to pre-existing copyright protection.

1. Relationship with intellectual property

The law of intellectual property recognises the fundamental tension that exists between the interests of society and the interests of the individual in the context of information dissemination.[197] Society has a legitimate interest in the free flow of and access to information.[198] In this vein, intellectual property is premised on the instrumental justification that its protection encourages the production and dissemination of valuable information that would not have otherwise reached the marketplace.[199] Intellectual property laws encourage the production and dissemination of information by granting rights of exclusivity that prevent information-creators from being undercut by competitors who have not borne the costs of creation.[200] As a result, the law of intellectual property must be seen as a self-contained body of law that maintains a delicate balance between the conflicting interests of society and individuals.[201] Parliament has established the appropriate remedies for breaches of intellectual

[197] Green, above n 23, at 206: "Intellectual property law is designed to balance the economic interests of creators in reaping the rewards of their efforts against those of society in having access to a free flow of new ideas."
[198] *Dixon* above n 1 at [34]: "the central concern is that affording confidential information the full protection of the property law would have a damaging effect on the free flow of information and freedom of speech. See also Weinrib, above n 24, at 149: information is as an "invaluable social resource"; Grant Hammond "Theft of Information" *The Law Quarterly Review* (1984) at 263: information is properly seen as an evolutionary social process rather than as a thing or a commodity.
[199] Brad Sherman and Lionel Bently *Intellectual Property Law* (2nd ed) (Oxford University Press, Oxford, New York, 2004) at 3.
[200] Ibid.
[201] Weinrib, above n 24, at 149: it has been argued that "the established body of rules governing intellectual and industrial property creates a careful balance between the interests of information owners and the interests of others," and recognising information as property tilts "the balance in favour of owners to the detriment of social interests."

property laws and attached them to the relevant statutes. Copying another's work, for example, is an infringement of copyright, which is governed by the Copyright Act 1994,[202] rather than constituting the theft of information. Copyright and theft are conceptually distinct and the appropriate rights and remedies have been established separately for each. Recognising property rights in information threatens to undercut this legislative framework. On this point, Grant Hammond has observed that:

> the commonwealth jurisdictions have a formal system of intellectual and industrial property laws, laid down by statute. Under those statutes, ideas or information as such are not legally protectable. However, limited forms of protection are granted to new and useful inventions, and literary and artistic creations. Even then, monopolistic or predatory behaviour is controlled. If an excess accumulation of market power occurs antitrust, or anticombines, or restrictive trade practices law may be employed to attack that concentration.[203]

The point here is that the legislature has struck a careful balance through the enactment of various statutes to ensure that the "invaluable social resource"[204] of information is utilised in the interests of society as a whole. Recognising property in information leads to individuals gaining dominion over information and "upsets [this] balance".[205] Accordingly, the criminal law must identify a transgression separate from the unauthorised copying of information before it imposes criminal liability. The following discussion identifies the legitimate grounds for criminalising the unauthorised copying of a computer file.

2. Trade Secrets

Confidential commercial information has been recognised by the criminal law as requiring protection beyond that afforded by intellectual property.[206] The additional criminality involved in taking a trade secret involves the violation of secrecy. The point of copyright is to protect information even once it has entered the public domain.

---

[202] See Part 6 of the Copyright Act 1994.
[203] Hammond, above n 196, at 261.
[204] Weinrib, above n 24, at 149.
[205] Ibid at 148.
[206] Crimes Act, s 230.

However, copying something that is publicly available involves a lesser degree of culpability than deliberately obtaining information that has been actively kept secret. That is why commercial information must be "subject to all reasonable efforts to preserve its secrecy" before it qualifies as a "trade secret" warranting the protection of the criminal law.[207] A trade secret is the product of effort and expense and thus its possessor has a legitimate interest in protecting its confidentiality.[208] The wrong involved in taking a trade secret without authorisation was articulated by the United States Supreme Court in *International News Service v. Associated Press*.[209] In the words of the Court, the "defendant" who takes and sells material that has been acquired by someone else "as the result of organisation and the expenditure of labour and skill […] is endeavouring to reap where it has not sown, and is appropriating to itself the harvest of those who have sown."[210]

The unauthorised taking of a trade secret is thus an evil legitimately warranting the protection of the criminal law. In *International News Service*, the law of property was employed to criminalise the misappropriation of the trade secret.[211] A similar level of protection, however, can be achieved through different means. Section 230 of the Crimes Act, aided by the broad definition of "document" in s 217, adequately protects against the unauthorised transmission of digital files containing trade secrets.[212] This is because under s 230(1)(a) it is an offence to dishonestly and without claim of right, take, obtain, or *copy* any document or any model or other depiction of any thing or process containing or embodying any trade secret, knowing that it contains or embodies a trade secret.[213] The duplicative nature of digital transmission means digital takings of trade secrets will always attract criminal liability under s 230. It is unnecessary, therefore, to elevate a computer file to the category of property in order to criminalise

[207] Ibid, s 230(2): "For the purposes of this section, 'trade secret' means any information that—
(a) is, or has the potential to be, used industrially or commercially; and (b) is not generally available in industrial or commercial use; and (c) has economic value or potential economic value to the possessor of the information; and (d) is the subject of all reasonable efforts to preserve its secrecy."
[208] Weinrib above n 24 at 143.
[209] *International News Service v. Associated Press* 63 L.ed. 211 (1918).
[210] Ibid at 221.
[211] Ibid. There are a number of American decisions that have treated information as property. See *U.S. v Bottone* 365 F.2d 389 (1966); *U.S. v Lambert v. Lambert* 18 U.S.C.A 641 (1970); *U.S. v. Girard* 601 F.2d 69 (1979); *U.S. v. May* 625 F.2d 186 (1980). For an argument in favour of recognising property in information on the basis of an expenditure of mental or physical effort see D.F. Libling "The Concept of Property: Property in Intangibles" (1978) 94 *Law Quarterly Rev.* 103-119.
[212] See discussion on pages 31-32.
[213] Crimes Act, s 230(1)(a) (emphasis added).

the misappropriation of sensitive commercial information. The Crimes Act adequately targets the misappropriation of digitised trade secrets without invoking the policy concerns that would accompany the admission of information to the category of property.

3. Computer misuse

A further legitimate ground for criminalisation is the protection against computer misuse.[214] Parliament has recognised that there is a "public interest in encouraging the use of computers and appropriate standards for users of computers."[215] Accordingly, protection against unauthorised interferences with an individual's computer is a legitimate basis for criminalisation. Section 252 achieves this objective by making every one liable to imprisonment who:

> intentionally accesses, directly or indirectly, any computer system without authorisation, knowing that he or she is not authorised to access that computer system, or being reckless as to whether or not he or she is authorised to access that computer system.[216]

Section 252, therefore, plays a vital role in criminalising unauthorised interferences with a computer because it is irrelevant whether there is any damage to the computer system itself or whether any data is abstracted.[217] Section 252 provides, therefore, a base level of protection to the possessors of digital data by criminalising *any* unauthorised access of a computer. The provision carries a maximum sentence of two years imprisonment and thus reflects the seriousness with which the law treats computer misuse.

Further, as already discussed, the breadth of "benefit" in s 249 allows the Crimes Act to criminalise the unauthorised abstraction of data from a computer system regardless

[214] The Court of Appeal in *Dixon*, above n 1, recognised this legislative aim at [39].
[215] Law Commission Computer Misuse (NZLC R54, 1999) at xi.
[216] Crimes Act, s 252(1).
[217] There is a degree of equivalence between certain more traditional property offences and those to be found in the computer crimes part of the Crimes Act in that s 249 mirrors s 231 (burglary), while s 252 is similar to s 29 of the Summary Offences Act.

of whether property rights subsist in the data itself.[218] Section 249 carries a maximum penalty of seven years imprisonment mirroring the maximum sentence available in the context of theft.[219] It is submitted, therefore, that the Crimes Act adequately criminalises computer misuse, including the unauthorised abstraction of data, without the inclusion of computer data within the criminal definition of "property".

4. Privacy

The sections of the Crimes Act dealing with computer crimes, particularly through s 252, recognise the invasion of privacy that accompanies accessing a computer without authority. The criminal law, through Part 9A of the Crimes Act,[220] also recognises a more serious invasion of privacy.

Part 9A criminalises the taking of [221] and any subsequent dissemination[222] of "intimate visual recordings," which is defined broadly to include any form of nudity or sexual activity.[223] Parliament has appropriately recognised that these acts involve a serious wrong legitimately attracting the official censure of the criminal law. Importantly, the criminal law recognises that an interference with property rights is not the relevant issue. Rather, it is the violation of an individual's private sphere that is the particular wrong justifying the censure of the criminal law. Accordingly, it is unnecessary to elevate a computer file to the category of property to criminalise this particular interference with someone's privacy through the unlawful obtainment of digital files.

5. Conclusion

The foregoing analysis reveals that the Crimes Act criminalises unauthorised obtainments of computer files when there are legitimate reasons to do so. These reasons do not rely on property rights subsisting in electronic data. Some obtainments of

[218] See discussion on pages 41-43.
[219] Crimes Act, s 223.
[220] Crimes Act, Part 9A: "crimes against rights of privacy."
[221] Section 216H prohibits the making of any intimate visual recording without the knowledge and consent of the subject of the recording.
[222] Section 216J then criminalises any subsequent publishing, importing, exporting or selling of the intimate visual recording.
[223] See Crimes Act, s 216G.

computer files are legitimately made criminal because there are other wrongs warranting criminal liability.

D Potential inconsistencies or absurdities

The main thread of the preceding discussion has been that the Crimes Act achieves its legitimate objectives without including a computer file in its definition of property. It remains to be determined, however, whether there are any inconsistencies and absurdities resulting from the exclusion of a computer file from the criminal definition of "property". On this point, the Court of Appeal in *Watchorn* added the following postscript to its judgment:

> the decisions of this Court in *Dixon* and the present case have identified some drafting issues and inconsistencies in some Crimes Act provisions. We respectfully suggest that consideration be given to remedial legislation.[224]

The Court did not actually say what exactly these drafting issues and inconsistencies were. Accordingly, these must be identified independently.

1. Receiving

One possible inconsistency resulting from the exclusion of computer files from the criminal definition of property relates to the crime of "receiving" codified in s 246. Subsection (1) of that provision provides the following:

> Every one is guilty of receiving who receives any property stolen or obtained by any other imprisonable offence, knowing that property to have been stolen or so obtained, or being reckless as to whether or not the property had been stolen or so obtained.[225]

This provision relies on the relevant subject matter coming within the criminal definition of "property". Accordingly, as it stands, a person who receives a copy of a computer file knowing it to have been obtained illegally will not face any criminal

[224] *Watchorn* above n 117 at [101].
[225] Crimes Act 1961, s 246.

liability. Recent events in New Zealand illustrate this issue. Political commentator Nicky Hager received digital information from a hacker with the alias "Rawshark", which Hager knew (or was at least reckless to the possibility) that it was obtained unlawfully.[226] However, to be a receiver under s 246, Hager had to be the recipient of "property". As Hager received digital data and not "property", he could not attract criminal liability.[227] If, however, Hager had received paper copies containing the same information then he could have faced liability as a receiver. As a matter of principle, it is perhaps illogical to allow a recipient to benefit from the spoils of a computer crime but criminalise the receipt of stolen property.

There exist, however, significant differences between receiving stolen property and receiving the spoils of a crime involving computers. In the latter case, the victim has not been deprived of his or her digital file. This is because digital information, like pure information, is a non-rivalrous good[228] and the crime of receiving is aimed at rivalrous goods where an original owner necessarily remains deprived of property through the act of receiving. In addition, digital data's capacity for infinite duplication means admitting electronic data to the category of property could result in a potentially overwhelming number of people facing liability as receivers. This could result in the over-criminalisation that both the Canadian Supreme Court and Elias CJ cautioned against.[229] On this basis, it is arguable that the costs of enforcement would significantly outweigh the social interest in criminalising this form of behaviour.[230] There are, therefore, material differences in the two receipts. Accordingly, whatever moral culpability lies in exploiting the spoils of a computer crime, the foregoing reasons preclude the admission of computer data to the criminal definition of "property" to target this potential issue.[231]

---

[226] "Rawshark's" actions would be criminalised under s 252 as he or she dishonestly accessed a computer without authorisation as well as s 249 because he or she dishonestly accessed a computer to obtain a benefit (sensitive information).
[227] See Gregor Allan "Dicey Policy and Dirty Politics" *NewsLaw* 7 November 2014, 23.
[228] Above n 104.
[229] Above notes 29 and 30.
[230] Abraham Bell and Gideon Parchomovsky "A Theory of Property" 90 *Cornell L. Rev.* 531 (2005), 565: "The digital information revolution seems to suggest that an asset may cease to be a suitable subject of property law because of an increase in the cost of protecting it." See also "Exploitative Publishers, Untrustworthy Systems, and the Dream of a Digital Revolution for Artists," 114 *Harv. L. Rev*. 2438, 2455 (2001) (suggesting that "peer-to-peer file-sharing technology like Napster's demonstrates the implausibility of street-level enforcement of copyright law generally).
[231] An individual could, however, be a party to a primary offence committed under s 249 if he or she aided or abetted the commission of the offence in any way: s 66 Crimes Act.

2. Abstraction of data from a non-computer

The exclusion of digital data from the criminal definition of "property" does result in the position that unlawfully obtaining data from a computer is criminalised but unlawfully obtaining data from a storage medium, which does not qualify as a "computer,"[232] may not. To attract criminal liability the 'data thief' would need to form an intention to permanently deprive the owner of his or her storage medium.[233] Accordingly, the data thief who only takes a storage medium temporarily for the purpose of abstracting data and then returns it unharmed will likely evade criminal liability provided he or she did not obtain a "trade secret". This can be seen as the digital equivalent of the problem that arose in *Oxford v Moss*.[234] In that case, a student obtained a copy of an exam paper, memorised its contents, and then returned the paper. The court, after refusing to recognise property rights in the information itself, held that there had been no intention to permanently deprive the university of the physical paper and therefore no criminal liability could ensue.[235] Although there exists the possibility for private law remedies,[236] none of the provisions in the Crimes Act recognise this type of interference with the property rights inhering in the storage medium as criminal provided the data does not qualify as a "trade secret". Sections 249 and 252, by criminalising the unauthorised "access" of a computer, avoid the illogicality of the conclusion in *Oxford v Moss*.[237] The same illogicality is not, however, avoided in the case of a storage medium that does not qualify as a "computer".

It has not been the aim of this dissertation to suggest legislative amendment but nevertheless it is submitted that a possible solution to the problem is the enactment of

[232] Above n 141.
[233] Crimes Act 1961, s 219(1)(a): "Theft or stealing is the act of dishonestly and without claim of right, taking any property with intent to deprive any owner permanently of that property or of any interest in that property."
[234] Above n 9.
[235] Ibid.
[236] See discussion on pages 39-43.
[237] See JC Smith "Theft: Oxford v Moss" [1979] Crim LR 119 at 120 where the absurdity of the result in *Oxford v Moss* is forcefully demonstrated: "An examination question paper, the preparation of which can involve hours of work by several skilled persons, is a relatively valuable thing. To equate it with the piece of paper would be no more sensible than to equate a banknote with the piece of paper on which it is printed or a Rembrandt with the canvas on which it is painted. That which was valuable has been rendered useless and must be replaced by the use of more valuable time by the University's employees."

a specific provision directed at "accessing a storage medium for a dishonest purpose". This provision could mirror the wording of s 249 and simply substitute the term "computer system" with "storage medium", which could be defined to mean "any electronic, mechanical, electromagnetic, optical, or electro-optical instrument, apparatus, equipment, or other device that is used or is capable of storing data."[238] This provision would remove the absurdity identified above by extending criminal protection to an owner's right to exclude others from interfering with a storage medium. Critically, this approach would not invoke the normative concerns militating against recognising information as property.

E Conclusion

This chapter has analysed the interaction between the private law and the criminal law in order to identify the legal consequences of excluding computer data from the criminal definition of "property". It has been argued that the appropriate grounds for criminalisation do not stem from an interference with property rights in electronic data. Rather, they stem from interferences with the property rights inhering in storage mediums, the unauthorised obtainment of trade secrets and invasions of an individual's privacy. Accordingly, the legitimate interests of the criminal law are best served by excluding electronic data from the criminal definition of "property". As a final thought, it is submitted that the reason the Court in *Watchorn* referred to "drafting issues and inconsistencies" is somewhat attributable to the "intuitive response that in the modern age digital data must be property."[239] This intuition has obscured proper legal analysis because the Crimes Act does not make it clear that electronic data is excluded from the criminal definition of "property". Consequently, the prosecution's submissions in *Dixon* and *Watchorn* were argued on an improper basis. Once it is conclusively determined whether electronic data is included within the criminal definition of "property" – either by the Supreme Court or by Parliament - then the relevant submissions can be framed with reference to the wrongs warranting the imposition of criminal sanctions. Clarity on this point and the enactment of a provision targeting the

[238] This proposed definition is a modification of the definition of "interception device" provided by s 216A(1) of the Crimes Act 1961.
[239] *Dixon v R*, above n 1 at [21].

unlawful abstraction of data from storage mediums would go a long way to resolving the issues and inconsistencies referred to by the Court in *Watchorn.*

CONCLUSION

The ambition of this dissertation has been to demonstrate that the law of property, particularly in the context of the Crimes Act, rightly equates electronic data with the information it contains. Consequently, until such time as the common law recognises information as property, computer data does not qualify as "property" for the purposes of the criminal law. This thesis was first defended with reference to the concept of property. It is the criterion of transferability that militates against the recognition of property rights in computer data as distinct from the information it contains. In the context of a digital file, the proper relationship amenable to the laws of property is the relationship between an individual and the information contained on the file. The duplicative nature of digital transmission means electronic data should not qualify as tangible property despite its physical existence. The same thesis was then defended with reference to the statutory context and history within which the criminal definition of "property" must be viewed. It was argued that the relevant history and context evinces Parliament's intention to equate electronic data with pure information. Finally, the consequences of excluding electronic data from the definition of "property" in the Crimes Act were assessed in light of the legitimate grounds for criminalisation. It was argued that the exclusion of electronic data from the definition of property best serves the interests of the criminal law because this exclusion compels the identification of a wrong beyond the unlawful copying of information. It is these further wrongs that appropriately attract the interest of the State.

The elevation of electronic data to the category of property is therefore an unnecessary and undesirable measure. It would violate a coherent concept of property, upset the careful balance struck by the laws of intellectual property, and distort the legitimate justifications for the criminalisation of computer misuse. Accordingly, despite offending the allegedly "intuitive contention that in the modern age a computer file must be property,"[240] the Court of Appeal's decision in *Dixon* must be seen as correct in law. It is true that technology often outflanks existing legal principles but it is important not to undermine the integrity of these existing principles by reacting hastily

[240] Above n 239.

to technological advancement. It would be, therefore, a grave error for the Supreme Court to overturn the Court of Appeal's decision in *Dixon* and hold that electronic data does in fact qualify as property for the purposes of the Crimes Act 1961.

SELECT BIBLIOGRAPHY

CASES

New Zealand

Davies v Police CRI-2006-488-56, [2008] 1 NZLR 638 (HC)
Dixon v R [2014] NZCA 329, [2014] 3 NZLR 504
Dixon v R [2014] NZSC 151
Dixon v R [2015] NZSC Trans 9; SC 82/2014
Everitt v Martin [1953] NZLR 298
Hosking v Runting [2004] NZCA 34, [2005] 1 NZLR 1
Hunt v A [2007] NZCA 332, [2008] 1 NZLR 368
Money Managers Ltd v Foxbridge Trading Ltd HC Hamilton CP67/93, 15 December 1993
P v T [1998] 1 NZLR 257 (CA)
Pacific Software Technology v Perry Group Ltd (2003) 7 NZBLC 103,950 (CA)
Police v Le Roy HC Wellington CRI-2006-485-58, 12 October 2006
R v Cox (2004) 21 CRNZ 1 CA
R v Dixon DC Invercargill CRI-2011-059-1122, 2 August 2013
R v Wilkinson [1999] 1 NZLR 403 (CA)
Taxation Review Authority 25 [1997] TRNZ 129
Watchorn v R [2014] NZCA 493

United Kingdom

Boardman v Phipps [1966] UKHL 2, [1967] 2 AC 46
Low v Blease (1975) 119 Sol J 695; [1975] Crim LR 513
Malone v Commissioner of Police (No 2) [1979] 2 All ER 624
National Province v Ainsworth [1965] UKHL 1, [1965] A.C. 1175
OBG Ltd v Allan [2007] UKHL 21, [2008] 1 AC 1
Oxford v Moss (1979) 68 Cr App R 183
Thurston v Charles 1905 21 TLR 659
Yearworth v North Bristol NHS Trust [2009] EWCA Civ 37, [2009] 2 All ER 986 (CA)

Australia

Farah Constructions Pty Ltd v Say-Dee Pty Ltd [2007] HCA 22
Kennison v Daire (1985) 38 SASR 404, 16 A Crim R 338
Kennison v Daire (1986) 160 CLR 129, 60 ALJR 249
Wilson v Marshall [1982] TasR 298

Canada

Stewart v R [1988] 1 SCR 963

United States

Hydro Res. Corp. v. Gray, 173 P.3d 749, 757 (N.M. 2007)

International News Service v. Associated Press 63 L.ed. 211 (1918)
South Central Bell Telephone Co. v. Sidney J. Barthelemy, et al. 643 So.2d 1240 (1994), 1246
U.S. v Bottone 365 F.2d 389 (1966)
U.S. v Lambert v. Lambert 18 U.S.C.A 641 (1970)
U.S. v. Girard 601 F.2d 69 (1979); *U.S. v. May* 625 F.2d 186 (1980)
Carpenter v United States 484 US 19 (1987)
People v Kwok 63 Cal App (4th) 1236 (1998)
People v Kozlowski 96 Cal App (4th) 853 (2002)

LEGISLATION

New Zealand

Crimes Act 1961
Crimes Amendment Act 2003
Commerce Act 1986
Consumer Guarantees Act 1993
Copyright Act 1994
Fair Trading Act 1986
New Zealand Bill of Rights Act 1990
Privacy Act 1993
Property Laws Act 2007
Sale of Goods Act 1908

United Kingdom

Theft Act (UK) 1986

United States

Mont Code Ann, s 45.2.101(54)(k) (1981)

New Zealand Bills

Crimes Amendment Bill (No 6) 1999 (322-1)

Law and Order Committee Crimes Amendment Bill (No 6)

REPORTS AND SUPPLEMENTARY ORDER PAPERS

Law Commission Computer Misuse (NZLC R54, 1999)

Supplementary Order Paper No 85 (20 July 2001)

BOOKS

Ackerman, Bruce *Private Property and the Constitution* (Yale University Press, New Haven and London, 1977)

Becker, Lawrence *Property Rights: Philosophical Foundations* (Routledge and K. Paul, London, Boston, 1977)

Berry, David *The Philosophy of Software* (Palgrave Macmillan, New York, 2011)

Finn, Jeremy and Robertson, Bruce (eds) *Adams on Criminal Law 2014 Student Edition* (Thomson Reuters, Wellington, 2014)

Green, Stuart *13 Ways to Steal a Bicycle* (Harvard University Press, Cambridge, Massachusetts, 2012)

Hohfeld, Wesley Newcomb *Fundamental Legal Conceptions as Applied in Judicial Reasoning*, ed. Walter W Cook and foreword Arthur L. Corbin (Greenwood Press, Westport, 1978)

Munzer, Stephen *A Theory of Property* (Cambridge University Press, New York, 1990)

Jackson, David *Principles of Property Law* (Law Book Co, Sydney, Melbourne, 1967)

Penner, James *The Idea of Property in Law* (Clarendon Press, Oxford, 1997)

Pretto-Sakmann, Arianna *Boundaries of Personal Property: shares and sub-shares* (Hart Publishing, Portland, 2005)

Sanders, Donald H *Computers Today* (McGraw-Hill, Singapore, 1988)

Underkuffler, Laura *The Idea of Property: Its Meaning and Power* (Oxford University Press, Oxford 2003)

Waldron, Jeremy *The Right to Private Property* (Oxford University Press, New York, 1988)

Wall, Jesse *Being and Owning* (Oxford University Press, Oxford, 2015)

Wasik, Martin *Crime and the Computer* (Oxford University Press, Oxford, 1991)

Worthington, Sarah *Equity and Property: Fact, Fantasy and Morals* (University of Queensland Press, Queensland, 2009)

TEXTBOOKS

Allan, Barry and Gault, Thomas *Gault on Commercial Law* (Thomas Reuters, Wellington, 2010)

Ashworth, Andrew *Principles of Criminal Law* (7th ed) (Oxford University Press, Oxford, 2013)

Bently, Lionel and Sherman, Brad *Intellectual Property Law* (2nd ed) (Oxford University Press, Oxford, New York, 2004)

Carter, A.T. Chalk, B.S. and Hind, R.W. *Computer Organisation and Architecture: An Introduction* (2nd ed.) (Palgrave Macmillan, Basingstoke, 2003)

Frankel, Susy *Intellectual Property in New Zealand* (2nd ed) (LexisNexis, Wellington, 2011)

Todd, Stephen (ed.) *The Law of Torts in New Zealand* (5th ed) (Brookers, Wellington, 2009)

Witting, Christian and Murphy, John *Street on Torts* (13th ed) (Oxford University Printing Press, Oxford, 2012)

JOURNAL ARTICLES

"Exploitative Publishers, Untrustworthy Systems, and the Dream of a Digital Revolution for Artists" (2001) 114 *Harv. L. Rev*. 2438

Bell, Abraham and Parchomovsky, Gideon "A Theory of Property" (2005) 90 *Cornell L. Rev.* 531

Green, Sarah "Rights and Wrongs: An Introduction to the Wrongful Interference Actions" in D Nolan and A Robertson (eds), *Rights and Private Law* (Hart Publishing, Oxford 2012) 538

Hammond, Grant "Theft of Information" *The Law Quarterly Review* (1984) 252

Honoré, A.M "Ownership," in A.G. Guest, ed. *Oxford Essays in Jurisprudence (First Series)* (Oxford, Clarendon Press, 1961) 107

Hostetler, Michael J "Intangible Property Under the Federal Mail Fraud Statute and the Takings Clause: A Case Study." (2000) *Duke LJ*. 589

Libling, D.F. "The Concept of Property: Property in Intangibles" (1978) 94 *Law Quarterly Rev.* 103

Mason, Stephen and Schafer, Burkhard "The Characteristics of Electronic Evidence in Digital Format" in Stephen Mason (ed) *Electronic Evidence* (3rd ed.) (LexisNexis Butterworths, London, 2012).

Ricketson, Sam "Confidential Information - A New Proprietary Interest? Part II (1977) *M.U.L.J*. 289

Saxer, Shelly Ross "The Fluid Nature of Property Rights in Water 21 (Fall 2010) *Duke Environmental Law & Policy Forum* 49

Smith, J.C. "Theft: Oxford v Moss" [1979] *Crim LR* 119

Arnold S. Weinrib "Information and Property" (1988) 38 *U.T.L.J.* 117

NEWSPAPER ARTICLES

Allan, Gregor "Dicey Policy and Dirty Politics" *NewsLaw* 7 November 2014, 23

ONLINE

Harvey, David "Digital Data and Theft – Collisions in the Digital Paradigm IV", July 29 2014 on "The IT Countrey Justice: An Occasional Blog about Law and IT": https://theitcountreyjustice.wordpress.com/2014/07/29/digital-data-and-theft-collisions-in-the-digital-paradigm-iv/.

Solum, Lawrence B. "Legal Theory Lexicon: Public and Private Goods," *Legal Theory Blog* (January 25, 2015): http://lsolum.typepad.com/legaltheory/2015/01/legal-theory-lexicon-public-and-private-goods.html.