Public Interest Law Journal of New Zealand

(2017) 4 PILJNZ 106

ARTICLE

Property or Not? Digital Files under the Criminal Law

KATHERINE HU*

The New Zealand Supreme Court in *Dixon v R* has recently ruled digital files to be "property" under s 249 of the Crimes Act 1961. However, this new definition may have much wider implications. For example, not only could it alter the traditional stance relating to the treatment of *information* under the law, but it also raises the issue of whether infringement of copyright could now attract criminal liability. This article discusses the recent developments in this area of law and contends that digital files should not be defined as "property" under the Crimes Act. Such an interpretation could undermine the application of well-established principles previously upheld by the Courts—a major concern is extending the criminal law too far, leading to over-criminalisation. The current state of the law has not adequately caught up to the advancement of modern-day technology. Rather than altering existing definitions under the Crimes Act, new and digital-specific solutions should be considered for dealing with legal issues arising from the digital world.

I Introduction

In an age where digital technology is developing rapidly, a significant concern is how the law should react to accommodate new areas of issue. Today, the real world comprises significant parts of intangible *digital-ness* because many things essential to daily life have been digitalised.[1]

The Crimes Amendment Act 2003 significantly updated pt 10 of the Crimes Act 1961, implementing many new computer-related offences. Recent case law has exposed areas

* LLB(Hons) student, University of Canterbury. The author would like to thank Professor Jeremy Finn of the University of Canterbury, Faculty of Law for his invaluable advice and supervision during the writing of the paper on which this article is based.

1 Moonho Song and Carrie Leonetti "The Protection of Digital Information and Prevention of Its Unauthorized Access and Use in Criminal Law" (2011) 28 John Marshall Journal of Computer and Information Law 523 at 523.

of uncertainty relating to these amendments and questioned whether they adequately cover the many situations resulting from the misuse of modern-day technology. The Supreme Court has "made a small dent" in the existing criminal law by holding that digital files are "property" for the purposes of the Crimes Act in *Dixon v R*.[2] This decision is particularly significant in the era of the Internet, or what has been described as "the age of 'hacked' or 'leaked' celebrity photos".[3] An example can be seen in the gaming context where in-game items can either be obtained in the course of gameplay or purchased with real world currency. These items are digital data or files loaded onto a player's account (database). And, as bizarre as it may sound to some, there are players who are willing to pay substantial amounts in exchange for these in-game items. For example, in 2013, an in-game "courier" item in the game Dota 2 was sold for USD 38,000.[4] A potential criminal issue in this context would be: what if someone hacked into a game account and thereby, dishonestly or by deception, and without claim of right, obtained these in-game items? There is little doubt that there would be an offence for unauthorised access under s 252 of the Crimes Act. However, the issue of how the criminal law should treat the digital files themselves is more uncertain. *Dixon* brought these issues into the spotlight; these issues are the focus of this article.

II Setting the Scene

While digital files, electronic files or computer files are somewhat comparable to hard-copy paper documents stored in physical folders, they are not quite as simple. Electronic files are a stored sequence of bytes; a byte is a unit of data comprising of eight binary digits which are essentially a code.[5] The code instructs a computer system to coordinate with a monitor or other output to express the file in a comprehensible form—for example, text, images or audio.

Under the Crimes Act, the term "document … in any form" covers documents in the form of electronic or digital files.[6] This was first accepted in the case of *R v Misic,* where it was argued that a program or disk did not amount to a "document" under the Act.[7] The Court held that, regardless of technological advancements, a document is "a document because there is a material record of information. This feature, rather than the medium, is definitive."[8] This is consistent with the extended definition subsequently enacted under the Crimes Amendment Act. But since "documents" were not expressly included in the Crimes Involving Computers provisions, the general position has been to argue digital files under the definition of "property".[9] Section 2 of the Crimes Act defines "property" as:

2 Kelly McFadzien and Tim Sherman "Digital files as property: a curious case in New Zealand" (2016) 13 Privacy Law Bulletin 71 at 71; and *Dixon v R* [2015] NZSC 147, [2016] 1 NZLR 678 [*Dixon* (SC)].

3 At 71.

4 Wesley Yin-Poole "Someone bought a Dota 2 courier for $38,000" (6 November 2013) Eurogamer <www.eurogamer.net>.

5 AT Carter, BS Chalk and RW Hind *Computer Organisation and Architechture: An Introduction* (2nd ed, Palgrave Macmillan, Basingstoke, 2003) at 2 and 10.

6 Section 217.

7 *R v Misic* [2001] 3 NZLR 1 (CA) at [35].

8 At [32].

9 See Crimes Act 1961, ss 248–254.

> ... 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 ...

Initially, the "presence or absence of an external thing" seemed to be of great importance for property rights to be attached.[10] This was because, on the one hand, it was believed that intangibles should not be "property" at all.[11] On the other hand, however, the traditional approach treated "property" as a very wide concept.[12] Prior to the amendments, s 217 of the Crimes Act provided that only "movable" objects were capable of being stolen. The major flaw of this definition was exemplified in *R v Wilkinson*, where it was held that electronically-transferred bank credit could not be stolen since it did not fall within the Act's (apparently) clear definition.[13] This prompted the Law Commission's *Computer Misuse* report which not only proposed an amendment to the term "property" but also recommended new provisions for computer-related offences.[14] Following this, in 2003, the Crimes Amendment Act was enacted.

The Amendment Act extended the definition of "property" in s 217 of the Crimes Act. The extension was, however, only made for electricity and money.[15] The addition of electricity supplemented the repeal of the old s 218 which made a separate offence for "abstraction of electricity".[16] This could be indicative of Parliament's view that general property-related offences were adequate for criminalising wrongful abstraction of electricity. Electronic files share many similarities to electricity, such as being comprised of electric signals and involving electric pulses when transferred. As "electricity" was included under the definition of "property" and digital data was not, one may presume that Parliament intended to exclude digital data. Moreover, the definition of "property" covers choses in action rather than intangibles in general.[17] Llewelyn and Low argue that this serves as a reminder that the law must administer accuracy and detail in protecting rights, particularly where the rights are abstract in nature, like that of most intangibles.[18] The Select Committee also rejected the Law Commission's proposed separate definition of "property". While some believed this was merely to avoid ambiguities within the Act, others such as David Harvey argued that it was a conscious decision to exclude the protection of digital data.[19] In another view, the statutory wording of the term "property" could also be construed to allow liberal interpretations and so be capable of covering digital files.[20]

10 David Llewelyn and Kelvin FK Low "Digital files as property in the New Zealand Supreme Court: innovation or confusion" (2016) 132 LQR 394 at 397.
11 James Penner and Henry Smith "Philosophical Foundations of Property Law" (Oxford University Press, Oxford, 2013) at 227.
12 See William Blackstone "Book 2: The Right of Things" in *Commentaries on the Laws of England* (Clarendon Press, Oxford, 1765).
13 *R v Wilkinson* [1999] 1 NZLR 403 (CA) at 410.
14 Law Commission *Computer Misuse* (NZLC R54, 1999) at [36].
15 Crimes Amendment Act, s 4(3).
16 Section 15.
17 Crimes Act, s 2.
18 Llewelyn and Low, above n 10, at 398.
19 See David Harvey "Theft of data?" (2014) 9 NZLJ 354 at 355.
20 Margaret Briggs "Criminal Law" [2015] NZ L Rev 115 at 116; and *Dixon* (SC), above n 2, at [11].

III The Orthodox Position

A Oxford v Moss

In this leading authority for the orthodox view, a university engineering student unlawfully obtained an examination paper, read it and then returned it.[21] The Court distinguished between the exam information (which was not property) and the paper medium (which was property). It held that the confidential information did not fall within the definition of "property" under the Theft Act 1968 (UK), so a conviction of theft was unable to be upheld.

B *Canada*

The *Oxford v Moss* approach was adopted in Canada in *R v Stewart.*[22] Here, the defendant counselled an employee of the Constellation Hotel to procure confidential information which the management department kept for payroll purposes. He was accordingly charged with counselling the commission of theft and fraud under the Criminal Code.[23] The issue before the Court was whether confidential information was capable of being property and therefore constituted "anything" under the Canadian offence of theft.

The trial judge originally found that confidential information was not property. The Ontario Court of Appeal overruled this and concluded that it was property. The importance of confidential information in society, and particularly in a commercial setting, formed the basis of this decision.[24] Notwithstanding, the Court of Appeal did restrict this application so that "such compilations will only be capable of being stolen if they are confidential".[25]

The Supreme Court reinstated the original decision on appeal. The Criminal Code required deprivation of any "property, money or valuable security" to be proven.[26] Also, since there had never been intentions to deal with the information commercially, the Court held that the hotel could not have been economically disadvantaged by the defendant's actions. The only "thing" that one could say was lost was confidentiality. The information was held to be something that was purely intangible so could only be converted and not taken. But "[s]ince there is no deprivation, there can be no conversion."[27] The judges further warned of the consequences which may result from any unwarranted extension of protection for confidential information:[28]

> For instance, the existence of such an offence would have serious implications with respect to the mobility of labour… Indeed, the realm of information must be approached in a comprehensive way, taking into account the competing interests in the free flow of information and in one's right to confidentiality or again, one's economic interests in certain kinds of information.

21 *Oxford v Moss* (1979) 68 Cr App R 183 (QB).
22 *R v Stewart* [1988] 1 SCR 963.
23 Criminal Code RSC 1985 c C-46, ss 283(1) and 338.
24 *Stewart*, above n 22, at 977–979.
25 At 971.
26 Criminal Code RSC 1970, c C-34, s 338(1); and *R v Olan* [1978] 2 SCR 1175 at 1178.
27 *Stewart*, above n 22, at 980.
28 At 978–979.

Finally, the Supreme Court carefully concluded that:[29]

> … if his interpretation was thought inadequate to meet the needs of modern society [particularly because its implication for the computer age], the remedy must be a change in the law by Parliament.

Subsequent cases in Canada have not only continued to re-affirm the *R v Stewart* position, but have also provided that where a tangible storage medium is the subject of theft, the value of the data, or files, contained on the medium will be considered.[30]

C *Australia*

Similar conclusions were drawn in Australia. For example, in *TS & B Retail Systems Pty Ltd v 3Fold Resources Pty Ltd (No 3)*, a case which involved claims over manufacturing drawings and data tables, it was held that confidential information was not property but rather something which was "protected by equity by 'the notion of an obligation of conscience arising from the circumstances in or through which the information was communicated or obtained'".[31]

D *New Zealand*

Traditionally, the New Zealand common law also followed *Oxford* by refusing to view information as property.[32] In *Taxation Review Authority 25*, a case involving the issue of whether computer programs and software amounted to "goods" under the Goods and Services Tax Act 1985, the Judge distinguished information from the instrument (such as a flash-drive) by which the information, or data, is carried.[33] This affirmed the orthodox position.

In *Watchorn v R*, an employee of TAG Oil (NZ) Ltd allegedly downloaded data from the company's computer system in anticipation of changing employers, but did not misuse the information.[34] He was initially convicted under s 249 of the Crimes Act, but this was overturned in the Court of Appeal where it was held that the information he had obtained was not property. It was submitted that the conviction be changed to "obtaining a benefit".[35] And while it was possible for this decision to have been decided under s 230 (taking, obtaining or copying trade secrets), provided that digital files are in fact treated as property, it is actually easier to bring cases under s 249 due to the additional actus reus required by s 230.[36]

---

29 At 968.

30 See *R v Desroches* (1992) 16 CR (4th) 182 (QCCA); *R v Cromier* 2013 QCCA 1068; and *R v Maurer* 2014 SKPC 118.

31 *Moorgate Tobacco Co Ltd v Philip Morris Ltd (No 2)* (1984) 156 CLR 414 (HCA) at 438 as cited in *TS & B Retail Systems Pty Ltd v 3Fold Resources Pty Ltd (No 3)* [2007] FCA 151, (2007) 158 FCR 444 at [74].

32 *Money Managers Ltd v Foxbridge Training Ltd* HC Hamilton CP67/93, 15 December 1993.

33 *Taxation Review Authority 25* [1997] TRNZ 129.

34 *Watchorn v R* [2014] NZCA 493.

35 At [22]–[23].

36 Anna Kingsbury "Using the criminal law computer misuse provisions to protect confidential information" [2016] NZLJ 128.

IV *Dixon*—Departure from the Orthodox Position

A *Facts*

During the 2011 Rugby World Cup, at a bar in Queenstown, an English rugby player known for his marriage to a member of the royal family was filmed on CCTV socialising and leaving with a woman who was not his royal wife. Mr Dixon, a bouncer working at the bar, had a receptionist download the file containing the footage onto a reception computer (without affecting the copy on the CCTV system itself). He then had it transferred from the reception computer to his personal flash drive, and deleted the file from the computer. After Mr Dixon made a failed attempt to sell the footage to media, he publicly posted it to YouTube. He was subsequently charged under s 249 which reads:

> **249 Accessing computer system for dishonest purpose**
>
> (1) Every one is liable to imprisonment for a term not exceeding 7 years who, directly or indirectly, accesses any computer system and thereby, dishonestly or by deception, and without claim of right,—
>
> (a) obtains any property, privilege, service, pecuniary advantage, benefit, or valuable consideration …

The trial judge held that the digital file was property under the Crimes Act, therefore convicting Mr Dixon under s 249.

B *Court of Appeal*

On appeal, the Court of Appeal held that "electronic footage stored on a computer is indistinguishable in principle from pure information", and "if confidential information is not property digital footage cannot be".[37]

The main point argued was that the refusal to include a separate definition in the Crimes Act was hugely indicative against any parliamentary intention to include digital files as property.[38] In its reasoning, the Court of Appeal distinguished the case of *Davies v Police* where a defendant downloaded pornography using his employer's Internet.[39] Unlike digital files, Internet usage was held to be "property" because usage of Internet involves consumption of megabytes in transmitting electronic data, which is separate and distinct from the information in the data itself. *Oxford v Moss* was also acknowledged as good law on the basis that it had been consistently followed and adopted in New Zealand and other jurisdictions.[40] The Court of Appeal endorsed equitable causes of action for the breach of confidential information; civil cases from other common law jurisdictions also support this approach.[41] For example, in *Boardman v Phipps* Lord Upjohn held that information was not property, but rather something "normally open to all who have eyes to read and ears to hear".[42]

---

37 *Dixon v R* [2014] NZCA 329, [2014] 3 NZLR 504 [*Dixon* (CA)] at [31] and [32].

38 See Crimes Amendment Bill (No 6) 1999 (322-1); and Supplementary Order Paper 2001 (85) Crimes Amendment Bill (No 6) 1999 (322-1).

39 *Davies (Daniel) v Police* [2008] 1 NZLR 638 (HC) at [1].

40 *Dixon* (CA), above n 37, at [25].

41 At [26]. See also *Boardman v Phipps* [1967] 2 AC 46 (HL); *Hunt v A* [2007] NZCA 332, [2008] 1 NZLR 368; and *Farah Constructions Pty Ltd v Say-Dee Pty Ltd* [2007] HCA 22, (2007) 230 CLR 89.

42 *Boardman*, above n 41, at [127].

The Court was of the view that relevant property rights attached to the digital file were the "exclusive possession and control" of the footage. Because the file was not deleted, it did not amount to a loss of the exclusive right to possession and control (that is, the property right). Still, it was held that the footage is different from the file itself—it is essentially information which the file holds—and since there is no "physical" thing which the right can be attached to, it cannot be property. This is slightly analogous to a United Kingdom case, *Malone v Commissioner of Police of the Metropolis*, where Mr Malone claimed he had property rights over conversations through telephone lines. The Court rejected his argument and ruled that the physical realisation of information through pulses of electricity could not give rise to property rights.[43]

The Court of Appeal also examined possible differences between digital data and confidential information. It was accepted that since a medium containing information could be property, it was possible for digital files to be property while the information contained by it was not.[44] This was supported by the previous authority of *R v Cox* which held that digital files have "a physical existence even if ephemeral".[45] This meant it was at least debatable that electronic files physically existed in a way that pure information does not. Still, the Court of Appeal decided that digital files could not be differentiated from the concept of pure information. It was considered to be:[46]

> … problematic to treat computer data as being analogous to information recorded in physical form. A computer file is essentially just a stored *sequence of bytes* that … cannot meaningfully be distinguished from pure information.

The Court also believed that policy concerns outweighed reasons for treating information in the form of digital files as property. And, although the Court accepted that the definition of property will change over time, it was of the view that Parliament would have specifically made the change if it had intended to do so.[47] It was contended that the original trial decision had only been reached as "an intuitive response that in the modern computer age digital data must be property".[48] Section 230 (taking, obtaining, or copying trade secrets) also supported the Court of Appeal's decision as it would become an unnecessary provision if confidential information were to be considered property. It was also noted that the Court's decision would not render s 249 a useless provision as it would still apply if a person had accessed a computer system and used credit card details to obtain goods unlawfully.[49] Thus, it was concluded that digital files were not property and Mr Dixon was instead charged with obtaining a "benefit" (see para VI for "benefit"). Mr Dixon appealed.

C *Supreme Court*

The Supreme Court overruled the Court of Appeal's decision, holding that digital files were in fact property for the purposes of s 249.[50] This decision is one of significant importance for a number of reasons.

---

43 *Malone v Commissioner of Police of the Metropolis* [1979] Ch 344.
44 *Dixon* (CA), above n 37, at [30].
45 *R v Cox* (2004) 21 CRNZ 1 (CA) at [49].
46 *Dixon* (CA), above n 37, at [31].
47 At [35].
48 At [20].
49 At [37].
50 *Dixon* (SC), above n 2, at [25].

First, while the Supreme Court expressly noted that it did not set out to reconsider the orthodox view of *Oxford v Moss*, it is difficult to see how the two decisions could sit harmoniously.[51] The *Oxford v Moss* decision creates a position in which the information on an examination paper is worthless. This is quite "odd" since the information (exam questions prepared with the time and labour of professors/lecturers) printed on the paper is what makes it valuable.[52] Similarly, the digital file Mr Dixon obtained would be totally worthless if it were not for the footage (information) it contained. So while it is clear in both cases that the information is the "thing" which contains value, only the court in *Dixon* recognises this by allowing protection under the criminal law. The Supreme Court also specifically pointed out academic criticism describing *Oxford v Moss* as "illogical and unprincipled", potentially indicating an indirect disapproval of the orthodox view.[53] Ultimately, departure from the orthodox view is an inevitable outcome of the Supreme Court's decision.

The Supreme Court accepted "property" as a term which does not have a precise meaning but rather a term which requires close examination of the statutory context.[54] Unlike similar cases arising in overseas jurisdictions, *R v Dixon* arose under computer-related provisions of the Crimes Act rather than general theft provisions. This context therefore allows a different interpretation of "property" so as to include digital files. However, since the Supreme Court considered the term "property" to encompass a broad scope, it is also likely that the *Dixon* decision in fact extends the general term of "property" under s 2.[55] This would follow to affect all offences under the Crimes Act. For example, it would then be possible for a person who, intentionally or recklessly and without clam of right, corrupts a digital file to be liable of an offence under s 269 for intentional damage. Such far-reaching extensions should arguably only be allowed under an express act of parliament.

The argument in the Supreme Court was that digital files are not simply information. Digital files were considered property because, as the Court summarised:[56]

> … digital files can be identified, have a value and are capable of being transferred to others. They also have a physical presence, albeit one that cannot be detected by means of the unaided senses.

With respect, however, this reasoning is unconvincing and has even been described as containing "numerous leaps of logic".[57] First, in the leading case of *National Provincial Bank Ltd v Ainsworth*, Lord Wilberforce defined "property" with a number of necessary characteristics: "it must be definable, identifiable by third parties, capable in its nature of assumption by third parties, and have some degree of permanence or stability".[58] The *Dixon* reasoning above only raises the attribute of being identifiable. Not only is this merely one of the many necessary attributes, it is not an attribute specific to property (evidently, just because a person can be identified does not mean they are property). Thus,

51 At [24].
52 Anirban Mazumdar "Information, Copyright and the Future" (2007) 29 EIPR 180.
53 JC Smith "Theft: Oxford v Moss" [1979] Crim LR 119 at 120 as cited *Dixon* (CA), above n 37, at [33] as cited in *Dixon* (SC), above n 2, at [20].
54 *Dixon* (SC), above n 2, at [25]; and *Kennon v Spry* [2008] HCA 56, (2008) 238 CLR 366 at [89].
55 *Dixon* (SC), above n 2, at [11], [34] and [46].
56 At [25].
57 Llewelyn and Low, above n 10, at 395.
58 *National Provincial Bank Ltd v Ainsworth* [1965] AC 1175 (HL) at 1247–1248.

being capable of being identified is hardly a convincing point for digital files to be treated as property.

Initially, the Supreme Court appeared to accept the physical-ness argument contained in the United States *South Central Bell Telephone Company v Barthelemy* case.[59] There, software was considered physically recorded knowledge which had a physical existence on a physical storage device and was therefore tangible personal property. Subsequent cases in the United States also made similar rulings.[60] Correspondingly, in *R v Cox*, New Zealand also accepted digital files as physical things.[61] Putting two and two together, it seemed sensible to follow this line of logic and conclude that digital files are physical things which should be treated as property. But, in the more recent case of *Thyroff v Nationwide Mutual Insurance Co*, the United States Courts considered electronic databases as "pure intangibles", and the basis for treating digital files as property shifted to their economic value.[62] However, believing that anything with economic value equates to property is flawed logic. Quite obviously, not all things with value are subject to property rights. For example, an "option to purchase" is clearly quite valuable but rather than property, it is a contractual right. As pointed out by Low and Llewelyn, the value of property is sometimes attributed to something which the property indirectly supplies but the property rights do not protect, for example paying extra for a view attached to a house.[63] Additionally, another "thing" of the digital world the law has had trouble catching up with is digital currency. It has been asserted that the protection of digital currency should not depend on the law but rather the programming codes and databases systems underlying its security (blockchain programming).[64] Even though the same protection systems or codes do not (and could not in a practical way) exist for digital files, the point is that the best method of protection may not be for digital files to be treated as "property".

Value-based arguments aside, the Supreme Court's ruling that "there seems to be no reason to treat data files differently from software" is still difficult to accept. The Court referred to other legislative contexts to support their argument, and it was found that "computer software" fell within the definition of "goods" (which means personal property of any kind)[65] under many consumer statutes.[66] But whether the term "software" includes data and files was not clear. Allan and Gault, for instance, advanced that there is "an important distinction between software and data".[67] Such a distinction would strongly go

59 *South Central Bell Telephone Co v Barthelemy* 643 So 2d 1240 (La 1994) at 1246.

60 See *Wal-Mart Stores Inc v City of Mobile* 696 So 2d 290 (Ala 1996); *American Business Information Inc v Egr* 264 Neb 574, 650 NW 2d 251 (Neb 2002); and *Andrew Jergens Co v Wilkins* 109 Ohio St 3d 396, 2006-Ohio-2708, 848 NE 2d 499 (Ohio 2006) at 57.

61 *Cox*, above n 45, at [49].

62 *Thyroff v Nationwide Mutual Insurance Co* 460 F 3d 400 (2nd Cir 2006).

63 Llewelyn and Low, above n 10, at 396.

64 Tatiana Cutts "Bitcoin Ownership and its Impact on Fungibility" (14 June 2015) CoinDesk <www.coindesk.com>.

65 Crimes Act, s 2.

66 See, for example, Consumer Protection (Definitions of Goods and Services) Bill (154-2) (select committee report) at 4. The Bill has been enacted as the Commerce Amendment Act 2003, Consumer Guarantees Amendment Act 2003, Fair Trading Amendment Act 2003 and the Sale of Goods Amendment Act 2003. They amended the definition of "goods" in the Commerce Act 1986, Consumer Guarantees Act 1993, Fair Trading Act 1986 and Sale of Goods Act 1908 to include computer software.

67 Thomas Gault (ed) *Gault on Commercial Law* (online looseleaf ed, Thomson Reuters) at [3A.2.03(1)(c)].

against treating electronic data or files the same as software, and therefore also go against the Supreme Court's conclusion.

The Supreme Court further noted that the United Kingdom had continued to uphold the *Oxford v Moss* approach. In *Your Response v Datateam Business Media*, the issue concerned whether an electronic database could give rise to or support a lien.[68] The answer was no. This was based on the nature of liens. Since digital databases were considered "intangible" property, they was incapable of forming a subject matter in tort that could be interfered with or possessed.[69] The United Kingdom Court of Appeal held that there was a bright line between the information itself and the physical storage medium.[70] Allowing a lien to arise in such a situation would therefore be contradictory to the traditional unwillingness to treat information as property, as shown in *OBG Ltd v Allan.*[71] Notwithstanding, the above United Kingdom decisions turned on the concept of exclusive possession while *Dixon* did not (both Mr Dixon and the original owner had possession or control over the same files). And for that reason, *Dixon* can be justifiably distinguished. There is also contradiction between United Kingdom legislation and case law. The fact that the United Kingdom Computer Misuse Act 1990 criminalises the interference with information makes it illogical for the orthodox position to reject criminalising dishonest obtaining of information, which is just another method of dealing with information.[72] This inconsistency therefore makes New Zealand's departure from the traditional position seem reasonable.

D *Possible consequences of the Supreme Court decision?*

If digital files are indeed "property" as the Supreme Court has concluded, there could be an extension of criminal responsibility to those who then download or republish them. For example, anyone who knowingly or recklessly downloads a hacked digital image of a celebrity would be at risk of both a criminal conviction and a maximum of seven years imprisonment under s 246.[73] This opens the door for incriminating anyone who receives hacked digital files. And since accessing and sharing digital files is so easy, this could lead to "over criminalisation".[74]

The Supreme Court's decision has also potentially "put the law significantly out of step with technology".[75] The nature of digital files means transfers can only be done through copying. So *Dixon* has indirectly brought the "copying" of digital files into the criminal scope of "obtaining property" while *other* forms of copying would not have similar criminal liabilities attached. For example, person A "owns" a digital image on their computer: in one situation person B transfers the digital image onto their own device, while in another situation person C takes a photograph of the digital image from their own device. The *Dixon* authority tells us (assuming all mental elements are present) that person B would be criminally liable for his actions while person C would likely not. This does not seem right as both would have essentially obtained the same material.

---

68 *Your Response Ltd v Datateam Business Media Ltd* [2014] EWCA Civ 281, [2015] QB 41 at [34].
69 At [17].
70 At [42].
71 *OBG Ltd v Allan* [2007] UKHL 21, [2008] AC 1 at [275].
72 Colin R Davies "Protection of Intellectual Property — A Myth? A Consideration of Current Criminal Protection and Law Commission proposals" (2004) 68 JCL 398.
73 Crimes Act, s 246.
74 *Dixon v R* [2015] NZSC Trans 9 at 46.
75 McFadzien and Sherman, above n 2, at 73.

A good case which could demonstrate the impact of the *Dixon* decision is one which was recently in the political spotlight: Nicky Hager receiving information from a hacker, going by the moniker Rawshark, for Hager's book *Dirty Politics: How attack politics is poisoning New Zealand's political environment*.[76] The Supreme Court's decision potentially "puts Hager back in the frame",[77] as Rawshark would be held to have obtained "property" as per s 249 and Hager, assuming the appropriate mens rea is present, would then have "received" this "property" under s 246.

V The On-going Debate

David Harvey supports the continuation of the orthodox position and has "no doubt that the decision of the Court of Appeal [was] correct technologically and in law".[78] He opined that while electronic files do in fact have a physical existence, they do not have a coherent form, since the nature of digital files make them difficult to be captured and maintained in their exact original form. While the information which we are able to view on a screen may appear unaltered, some of the essential "meta-data" tracing the file's history may have changed. And since such changes also take place during transfer, it is technically impossible to transfer the property rights of any exact digital file making it very difficult to classify it under "property". And unlike information presented on paper, the content of digital data alone does not inform as it is in a state which is "incoherent and incomprehensible" without the help of hardware and software.[79] Harvey believes it is dangerous to view the existence of digital data on a computer as analogous to that of information in a book because digital data does not, and cannot, exist without the hardware device which deciphers and presents it in a comprehensible way.[80]

Still, just because electronic data alone is something incomprehensible does not necessarily mean it is conceptually different from information on hard-copy paper—times have changed and realistically, everyone has some sort of access to electronic devices. And if Harvey's proposition is correct, absurd arguments—such as, encoded information on printed paper is not 'information' as it is incomprehensible—would become possible.

Further criticism of the Supreme Court's decision is that some aspects of the reasoning are hard to follow.[81] An example is the Court's discussion relating to the extended definition of "documents" under s 217. Since the term "document" is neither included in s 249 nor within the meaning of "property", the Court had no merit referring to it. The only way in which the reference may have been of help is perhaps if Mr Dixon had been charged under s 228 (dishonestly taking/using a document) instead. It is noted that while s 228 does not involve any computer-related elements, it does in fact carry the same maximum penalty as s 249. It is on that account (that s 228 could be a substitute) which

76 Nicky Hager *Dirty Politics: How attack politics is poisoning New Zealand's political environment* (Craig Potton, Nelson, 2014); and Paloma Migone "Crown admits breach in Hager search" (15 July 2015) Radio New Zealand <www.radionz.co.nz>.

77 David Fisher "Court decision puts Hager back in frame" *The New Zealand Herald* (online ed, Auckland, 28 October 2015).

78 Harvey, above n 19.

79 Burkhard Schafer and Stephen Mason *The Characteristics of Electronic Evidence in Digital Format* (3rd ed, LexisNexis, London, 2012) at [2.05].

80 Harvey, above n 19; and Schafer and Mason, above n 79, at [2.06].

81 Llewelyn and Low, above n 10, at 395.

commentators have suggested that the Supreme Court should not have "ventured into such controversial territory".[82]

Margaret Briggs provides another perspective. Briggs accepts possible "downstream effects" of allowing information to be regarded as property, noting the possible issues of copyright breaches mutating into a criminal offence under s 249. However, she also asserts concern over the law's awkward position of "trying to adhere to an analogue past, while operating in a digital here and now".[83] Digital information undoubtedly has a "market value" as it can be purchased, sold, licensed and dealt with in many ways that are similar to property. To say digital data cannot be "accessed" (and thus also cannot be taken, obtained, stolen, received) like property may not make sense—this is particularly true in today's society where a majority of important information has been digitalised. On top of that, copyright and privacy remedies may not be available. Even if such remedies were available, it is entirely possible that the damages rewarded do not sufficiently compensate for the harm done. It is, therefore, quite tenable to say that the orthodox approach is outdated.

Briggs also considered a hypothetical scenario in which a person breaks into a house and steals a USB containing a digital file which is somewhat of value. Under the position that "digital files cannot be property", an offence of theft would only relate to the USB rather than what is stored in it.[84] In the old case of *R v Bennitt* the courts had to expressly distinguish between the physical paper a cheque was made on and the value which the paper symbolises.[85] Such a distinction between cheque and value may seem to be the straightforward and obvious answer, but is that not painfully similar to the distinction between digital file and USB?

Furthermore, many types of digital files in the form of recordings are already protected under civil law legislation.[86] For that reason, the extension of criminal responsibility to include digital files in *Dixon v R* can be conceived as "reinforcing existing legal protections" and is a decision which is "consistent with the civil law protection already in place over misuse of digital content".[87] However, the opposite argument is just as tenable—it could be said that the current civil law sufficiently provides for digital data and the *Dixon* extension is unnecessary.

The legislative wording "accessing computer systems" in s 249 has also been asserted to be strongly indicative against the intention for electronic data to be considered as property.[88] Section 248 provides that "access" also means to "instruct, communicate with, store data in, receive data from, or otherwise make use of any of the resources of the computer system". It was advanced that this would create a "nonsensical tautology" within the Act—if "access" in s 249 was replaced with "receive data from" and "property" replaced with "data", the section would read, "…receive data from any computer system and thereby obtains any data". While there is sense in the forgoing argument, this writer is of the view that the alterative nature of the s 248 interpretation of "access" (use of the word

82 At 399.
83 Briggs, above n 20, at 120.
84 At 121.
85 *R v Bennitt* [1961] NZLR 452 (SC).
86 See, for example, Privacy Act 1993, ss 2 and 42; and Official Information Act 1982, ss 2 and 16.
87 Charles Mabbett "Supreme Court says digital files are property" (23 October 2015) Office of the Privacy Commissioner <www.privacy.org.nz>.
88 Lance Green "Does the definition of 'Property' in the Crimes Act 1961 include electronically stored data? The computer says 'No'." (LLB (Hons) Dissertation, University of Otago, 2015) at 31.

"or" in the provision) could also be argued as allowing the term to encompass a range of meanings rather than restricting the coverage which the term "property" provides.

VI Possible Solutions?

It is consistently and undoubtedly recognised that, notwithstanding whether digital files are to be viewed as property or not, Mr Dixon should be subject to some sort of criminal liability—the only issue is *what* it should be.

In the words of the Law Commission, perhaps "the importance of information as a business asset in the knowledge economy may justify redefinition of information as a property right for both civil and criminal law purposes".[89] However, classifying digital files as property still has a real potential to adversely affect the free flow information. Chief Justice Elias voiced concerns of "over criminalization",[90] and commentators similarly expressed the "risk that enforcement may be excessive or based on an inexpert understanding of the nature allegedly taken".[91] Lamer J made an example of such concerns in *Stewart*, where a person who happens to remember some sort of valuable information could be susceptible to being charged with possession of stolen information "each day that he is unable to forget the information".[92] With respect, however, this concern is overstated or even "far-fetched" and "somewhat fanciful".[93] This is attributed to the fact that such a conviction would be very difficult to uphold, given the near impossibility for proving possession if an offender had done nothing more than remember information.

McFadzien and Sherman have suggested that the Courts overrule its own decision.[94] If the law were to backtrack, digital files would likely be categorised under the term "benefit" instead. The definition of "benefit" would, therefore, be central to the actions which are criminalised under s 249. The Supreme Court's final conclusion assumedly did not affect the "benefit" interpretations of the Court of Appeal. The Supreme Court briefly and liberally construed the term to cover the "opportunity to sell footage", while the Court of Appeal held that "benefit" was wide enough to uphold a conviction under s 249.[95] *Watchorn* further held that there were no grounds to restrict "benefits" to financial advantages or the ordinary meaning of anything that is advantageous to the person involved.[96] In *Police v Le Roy*, the definition was extended to include the "acquiring of knowledge or information which one was not otherwise entitled".[97] Section 238 further provides added ground for the broad interpretation of "benefit"—the intentional absence of the term "benefit" in this provision indicates that the section was intended to be solely concerned with only financial advantages, so any terms with connotations extending beyond are purposely excluded. The flaw of categorising digital files as a "benefit",

89 Law Commission, above n 14, at [36].
90 *Dixon*, above n 74.
91 Kingsbury, above n 36.
92 *R v Stewart*, above n 22, at 977.
93 David H Doherty "Stewart: When is a Thief not a Thief? When he Steals the 'Candy' but Leaves the 'Wrapper'" (1988) 63 CR (3d) 322.
94 McFadzien and Sherman, above n 2, at 73.
95 *Dixon* (CA), above n 37, at [39].
96 *Watchorn*, above n 34, at [81].
97 *Police v Le Roy* HC Wellington CRI-2006-485-58, 12 October 2006 at [11].

however, is evident in situations where someone takes a digital file with the intention of using it in a vengeful manner—it is hard to see how this could amount to a benefit.

It is recognised that the *Oxford v Moss* decision has been criticised as "illogical and unprincipled".[98] Not only was it an old decision (1978), it was also determined at a time when digital information was far less significant than it is today.[99] It is also argued that equating an exam paper—something quite valuable as it contains substantial work from the professors/lecturers involved—to the paper on which it is printed is analogous to equating a famous and valuable painting to the canvas on which it was painted.[100] This distinction between the medium and information indicates the worth of information to be dependent on a tangible form. This is a potentially flawed position to take, particularly in our modern world which is commonly labelled as an "information-based society". Great caution would therefore be recommended in following it. Accordingly, it is proposed that legislative action would perhaps be the better solution.

It may be tempting to just let Parliament amend the definition of property to include digital files/data. But it is evident that this would be a problematic step as it could hugely impact the free flow of information. Very careful restrictions would therefore be required, such as implementing a narrower scope of application, if an extended definition were adopted.

It has also been contended that there is no need for any extended definitions as the property rights associated with digital data are already appropriately protected by the private law. Intellectual property law,[101] for example, was "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".[102] Alternatively, a course of action under the law of tort could be available where someone directly interferes with a USB device containing a digital file in a way that results in trespass.[103] Moreover, the current Crimes Act provisions arguably already provide sufficient basis for the proper criminalisation of conduct when it comes to the "interests" or "rights" which electronic files/data may represent. This includes provisions relating to trade secrets,[104] privacy,[105] and computer misuse in general[106]—none of which depend on electronic files being treated as "property".

It is this author's view that none of the above suggestions adequately address the criminality of such conduct.[107] The new digital era heralds technology which is very different from what the law has previously dealt with. For the law to properly catch up and accommodate this new technology, it is only right that the criminalisation of conduct in relation to digital files is given a careful and specialised examination. In 1980, the Canadian Supreme Court stated that since computers were a new type of device, they should be

98 Harvey, above n 19, at [354]; *Dixon* (CA), above n 37, at [33]; and *Dixon* (SC), above n 2, at [20].
99 D Kelleher "Stealing Information" (2001) 2 Technology and Entertainment Law Journal 9.
100 Smith, above n 53, at 120.
101 See, for example, Copyright Act 1994.
102 Stuart P Green *13 Ways to Steal a Bicycle* (Harvard University Press, Cambridge (Mass), 2012) at 206.
103 See Stephen Todd (ed) *The Law of Torts in New Zealand* (7th ed, Brookers, Wellington, 2016) at [12.2].
104 Crimes Act, s 230.
105 Section 252. See also pt 9A.
106 Section 252. See also pt 9A.
107 See also Johnathan Clough "Data Theft? Cybercrime and the Increasing Criminalization of Access to Data" (2011) 22 Crim LF 145 at 149.

treated as such by the law.[108] This was a major catalyst for the first amendments to the Canadian Criminal Code. So perhaps this line of logic should also apply to digital files. This is because, even in keeping the position of *Watchorn* or the *Dixon* Court of Appeal's approach of classing digital data and files under "benefit", there is still the risk of uncertainty (see para VI). To avoid the difficulties discussed regarding the current positions, this author's view is that electronic data or files could be protected as a "thing" or "term" itself (as opposed to electricity which is regarded a thing which is sufficiently provided for under general theft offences). This could involve including the term "digital files" in s 248 and also inserting "digital files" into s 249. The difficulty would then be defining what exactly digital files or data would encompass, but the technical definition (see para II) may be acceptable. The recommended amendment could read:

> **249 Accessing computer system for dishonest purpose**
>
> (1) Every one is liable to imprisonment for a term not exceeding 7 years who, directly or indirectly, accesses any computer system and thereby, dishonestly or by deception, and without claim of right,—
>
> (a) obtains any *digital data*, property, privilege, service, pecuniary advantage, benefit, or valuable consideration …

On a slightly tangential note, it has been identified that digital files are still at risk where they are obtained from somewhere that is not a computer system but for instance, from a USB drive. A useful solution was suggested in an Honours dissertation by Lance Green from the University of Otago which involves a new offence directed towards "accessing storage mediums for dishonest purposes" drafted similarly to s 249, and the insertion of a clear definition for "storage medium".[109]

Finally, as highlighted in *Watchorn*, there are some obvious "drafting issues and inconsistencies in some Crimes Act provisions".[110] A specific example would be the s 246 offence of "receiving" a conviction which requires one to "receive… property". This means that if digital files were *not* "property", the actions of someone downloading a wrongfully obtained file could not be brought under receiving. If we compare a person receiving a stolen paper copy of a document with another person receiving a digital file (containing the exact same information) it seems fundamentally unfair and senseless to convict the former but not the latter when both are, arguably, equally culpable in that they have benefitted in a similar way. It follows that this writer agrees with the Court in *Watchorn* and recommends that "consideration [should] be given to remedial legislation".[111] A recommendation which could complement this writer's suggested model could be to implement a new "receiving" offence under the computer-related offences section for digital data, or even to amend s 246 to include digital files and data.

It is accepted that there are concerns about over-criminalisation, and therefore enforcement costs. This is because electronic data can be duplicated infinitely, so there is a very high potential for digital data which was originally obtained through a computer misuse offence to have a substantial amount of subsequent recipients.[112] Regardless, the writer submits that two things could alleviate this concern:

---

108 *R v McLaughlin* [1980] 2 SCR 331 at 341.
109 Green, above n 88, at 52.
110 *Watchorn*, above n 34, at [102].
111 At [102].
112 *Stewart*, above n 22, at 976–978; and *Dixon* (SC), above n 2.

(1) the offence's requisite mens rea elements of either knowledge or recklessness means that only the actions of only those who have the necessary knowledge or recklessness regarding the wrongful obtaining of the digital file will be incriminated; and
(2) in terms of enforcement costs, it is the view that if there are clear and proper provisions (and penalties) in place this would be a strong deterrent, thus decreasing the number of people who would knowingly or recklessly become recipients to wrongfully obtained digital files.

After all, most digital files (such as .mp3 audio files for music from famous artists, .mp4 files for Hollywood movies and .pdf for written articles.) that the general public choose to download through computers almost always contain some "value" (since people would have paid for the same thing if they were in the form of CDs, DVDs and books.). It is, therefore, fair to criminally sanction the wrongful obtaining and subsequent receiving of those digital files, as people should not be downloading electronic files they know (or are reckless as to whether they) have been illegally obtained.

VII Conclusion

This article has discussed many different approaches and considerations involving the legislative history, different statutory contexts, potential policy concerns and academic comments relating to the treatment of digital files. And, with the utmost respect, all of these eventually lead to the same conclusion that the Supreme Court's ruling—that digital files are property under the Crimes Act—was likely a mistake. The current law is not comprehensive enough to cater for the new issues posed by the digital world. The current law not only has trouble keeping up with the fast-paced development of the digital world, but it also does not reflect a good understanding of these advancements. This has either left gaps or created ambiguities in the system, particularly in the case of digital files or data. Therefore, there is much need for the holes to be filled and the inconsistencies to be amended. New concepts call for new solutions.

Whichever method is used to resolve this issue—whether Parliament decides to step in or the courts get another chance to consider this area of law—caution is required to avoid producing any of the outlined risks and undesirable outcomes. As the saying goes, good intentions do not always equal good results.