CASE NOTE: DIGITAL PROPERTY - *DIXON V R* [2015] NZSC 147, [2016] 1 NZLR 678

DAVID HARVEY*

I. INTRODUCTION

This article examines the Supreme Court decision of *Dixon v R* (*Dixon*).[1] It suggests that the Supreme Court characterisation of a digital file is wrong and is based on a number of incorrect assumptions and fallacies about technology. The decision demonstrates what can go wrong when Judges attempt to judicially legislate in the field of law and technology, and suggests that such policy matters should be left to the legislature.

II. THE FACTS

Mr Dixon, the appellant, had been employed by a security firm in Queenstown. One of the clients of the firm was Base Ltd, which operated the Altitude Bar in Queenstown. Base had installed a closed-circuit TV system in the bar.

In September 2011 the English rugby team was touring New Zealand as part of the Rugby World Cup. The captain of the team was Mr Tindall. Mr Tindall had recently married the Queen's granddaughter. On 11 September, Mr Tindall and several other team members visited Altitude Bar. During the evening there was an incident involving Mr Tindall and a female patron, which was recorded on Base's CCTV.

Mr Dixon found out about the existence of the recording of Mr Tindall and asked one of Base's receptionists to download it onto the computer she used at work. She agreed, being under the impression that Mr Dixon required it for legitimate work purposes. The receptionist located the file and saved it onto her desktop computer in the reception area. Mr Dixon subsequently accessed that computer, located the relevant file and transferred it onto a USB stick belonging to him.

Mr Dixon attempted to sell the footage, but when that proved unsuccessful he posted it on a video-sharing site, resulting in a storm of publicity both in New Zealand and in the United Kingdom. At his District Court trial, Judge Phillips found that Mr Dixon had done this out of spite and to ensure that no one else would have the opportunity to make any money from the footage.

A complaint was laid with the Police and Mr Dixon was charged under s 249(1)(a) of the Crimes Act 1961 (Crimes Act).

That section provides as follows:

> 249 Accessing computer system for dishonest purpose

* District Court Judge (retired).

[1] *Dixon v R* [2015] NZSC 147, [2016] 1 NZLR 678 [*Dixon* SC].

> (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 indictment against Mr Dixon alleged that he had "accessed a computer system and thereby dishonestly and without claim of right obtained property."

III. The Procedural History

The Judge at first instance considered that the digital CCTV files were property within the meaning of the definition of that word in s 2 Crimes Act. When the matter went before the Court of Appeal, the Court disagreed.[2] It concluded that digital information or a data file did not fall within the definition of property.

The Court of Appeal's decision was the subject of considerable critical comment. It was even suggested that the provisions of s 249 Crimes Act were "unfit for the purpose". Yet the decision should not have come as any surprise, for there is a substantial body of authority, primarily in the civil arena, that supports the Court's conclusion. Subsequently, the Court made a similar finding in the case of *Watchorn v R*.[3]

What the Court of Appeal did in *Dixon*, however, was to substitute another charge which could have been proffered against Mr Dixon – that he accessed a computer and dishonestly and without claim of right obtained a benefit. In its decision, the Court of Appeal went to some pains to consider the nature of a benefit and substitute it as the charge.[4]

Mr Dixon appealed against that conclusion to the Supreme Court of New Zealand. He represented himself before the Court. His argument did not concentrate on the issue of digital property, unlike the very full argument that was advanced by the Crown[5] and that was largely adopted by the Court.

IV. The Supreme Court Decision

In its decision, the Supreme Court concluded that the Court of Appeal's conclusion that a digital file did not amount to property was wrong. It quashed Mr Dixon's conviction for obtaining a benefit contrary to s 249(1)(a) Crimes Act and it reinstated his original conviction for obtaining property by accessing a computer system for a dishonest purpose. Phyrric victory does not adequately describe the outcome from Mr Dixon's point of view.

---

[2] *Dixon v R* [2014] NZCA 329, [2014] 3 NZLR 504 [*Dixon* CA].
[3] *Watchorn v R* [2014] NZCA 493.
[4] *Dixon* CA, above n 2, at [40]–[49].
[5] *Dixon* SC, above n 1, at 680–683.

A. Digital Property

The Court started by considering the provisions of s 249 of the Crimes Act 1961, along with the definitions of "access", "computer system"[6] and "property".[7]

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". The Court adopted the characterisation of the Crown of the definition as:

> (a) Inclusive rather than exclusive
> (b) Circular, in that property is defined as including "real and personal property"
> (c) In wide terms and includes tangible and intangible property.

The Court also noted, in particular, that digital material in the form of computer software was defined as "goods" for the purposes of the Commerce Act 1986, the Consumer Guarantees Act 1993, the Fair Trading Act 1986 and the Sale of Goods Act 1908.[8]

1. *The District Court Approach*

The Court also considered the approach of the District Court where Judge Phillips observed that:[9]

> I see that what a computer does is receives, digests and analyses data. I consider that data can include anything that is capable of being stored on a computer system, being a word document or a programme file or a script, that enables the operator to do something quickly for example and can clearly include picture files and the like.

2. *In the Court of Appeal*

This approach did not find favour with the Court of Appeal. The Court of Appeal's starting point was that digital files were not property within the meaning of the definition of the Crimes Act because they were pure information. The Court adopted what it described as an "orthodox" view that information, whether confidential or not, was not property.[10]

It observed that the medium upon which information could be stored would be property but the information upon it would not. Therefore, the digital "footage" could not be distinguished from information on this basis.[11] The Court observed that it was problematic to treat computer data as being analogous to information recorded in physical form. It observed that a Microsoft Word document may appear to be the

---

[6] Crimes Act 1961, s 248.
[7] Section 2.
[8] Now incorporated in the Contract and Commercial Law Act 2017, s 119.
[9] *R v Dixon* DC Invercargill CRI-2011-059-1122, 17 April 2013 at [13].
[10] *Dixon* CA, above n 2, at [29].
[11] At [30].

same as a visible sheet of paper containing text but in fact was simply a stored sequence of bytes.[12]

The Court then considered whether or not it should depart from this orthodox view, observing that the distinction drawn between information which was not property and the medium upon which it was contained had been criticised as illogical and unprincipled. The view was that there were certain policy reasons militating against the recognition of information as property particularly in that such a decision could impact detrimentally upon the free flow of information and the freedom of speech.[13]

The Court noted that when the legislature enacted the computer crime sections of the Crimes Act, there were also amendments to the definition of "property" but that these were limited. The taking of confidential information or trade secrets was encompassed by s 230 Crimes Act.[14] It considered that the provisions in s 249 relating to property were aimed at situations where a person accessed a computer and used, for example, a false or purloined credit card details to obtain goods unlawfully.[15]

3. *Watchorn v R*

Shortly after the Court of Appeal decision in *Dixon* the Court was confronted with a similar issue in *Watchorn v R* (*Watchorn*).[16] The accused had been convicted on three charges alleging breaches of s 249 of the Crimes Act and claiming that he had access to his employer's computer system and dishonestly or by deception and without claim of right obtained property. The property in question were computer files relating to oil exploration information gathered by the appellant's employer.

The Court of Appeal noted its decision in *Dixon,*[17] where it was held that digital CCTV footage stored on a computer was not "property" as defined in the Crimes Act and so the obtaining of such data by accessing a computer system could not amount to "obtaining property" within the meaning of s 249(1)(a) of the Crimes Act. The Court accepted that that analysis must apply to the kind of data obtained by Mr Watchorn and observed that it was bound to follow *Dixon*.

4. *Different Results in the Court of Appeal*

The Court of Appeal in *Dixon*, while holding that a digital file could not be property, decided that it could substitute a different charge – that of accessing a computer system to obtain a benefit, which was available pursuant to s 249 of the Crimes Act.

In *Dixon* the benefit had been the opportunity to sell a digital CCTV footage that had been obtained by accessing his employer's computer. In *Watchorn* there was no evidence that the appellant had tried to sell the data, but the issue was whether or

[12] At [31].
[13] At [33]–[35].
[14] At [37].
[15] At [38].
[16] *Watchorn v R*, above n 3.
[17] *Dixon* CA, above n 2.

not the word "benefit" was limited to a financial advantage or something wider. After considering authority, however, the Court concluded that it was not essential that the word "benefit" be linked to some form of financial advantage.

The Court concluded that the issue of what constituted a benefit in Watchorn's case was more nuanced than that of *Dixon*. The Court considered that it was arguable on the facts of Watchorn's case that the advantage that he gained was his ability to access the data outside his work environment and without the supervision of his colleagues, including after he had left his employment.[18]

Indeed, the Court said that it could be argued that he did not, in fact, exploit the advantage given to him by selling the data or making it available to his new employer. It did not, in fact, reduce the ability that he had to do any of those things.[19]

When it came to considering whether to substitute the charge – as had been done in *Dixon* - the problem was that the Crown did not actually formulate the nature of the benefit that Mr Watchorn might have received. The failure to articulate such a benefit meant that Mr Watchorn did not have any notice of that allegation that he could properly contest. The Court held that he was entitled to such notice.[20]

The Court considered that the evidence that could be adduced might include whether or not there was in fact any advantage to him in having possession or control of the data and because the prosecution had restricted its theory of the case to obtaining property, the entitlement that Mr Watchorn had to prior notice of the benefit was not present. Accordingly, the Court was not prepared to substitute new verdicts and indeed the grounds for substituting such verdicts were not met.[21]

B. In the Supreme Court

1. *Intangibles as Property – the Context Approach*

Against this background, the Supreme Court adopted an unusual approach. It decided that it would by-pass an examination of the "orthodox view" that information was not property. The reason for this was that the Crown had approached the argument on the basis that digital files were not information but were property in that they could be owned and dealt with like any other item of personal property.[22]

The Court then went on to suggest that the nature of property depended upon context.[23] The context in *Dixon* was that of the computer crimes provisions of the

[18] *Watchorn v R*, above n 3, at [83]
[19] At [83].
[20] At [85].
[21] At [86].
[22] *Dixon* SC, above n 1, at [23]–[24].
[23] At [25] (citing *Kennon v Spry* [2008] HCA 56, (2008) 238 CLR 366 at [89]: where it was stated that property "is not a term of art with one specific and precise meaning. *It is always necessary to pay close attention to any statutory context in which the term is used*" (emphasis added)).

Crimes Act. This meant that within the context of computer crimes and the dishonest acquisition of property (among other things) a digital file fell within the ambit of "property".[24] Before going on to a more detailed analysis of why the Court reached that conclusion, the Court summarised the reasons why it came to this conclusion. The files were identifiable, had value and were capable of being transferred. It was conceded that although they could not be detected by the unaided senses,[25] it mattered not that they were intangible because the definition in s 2 of the Crimes Act included intangibles within the definition of property.

The Court then went into more detail, tracing the legislative history of the computer crimes sections of the Crimes Act. It was observed that a proposed definition of property, which did not appear in the legislation as enacted, would have put the position of a digital file beyond question.[26]

2. *A Diversion to "Documents"*

Curiously enough the Court then went on to discuss the nature of a document and the extended definition of that term, drawing assistance from the decision of *R v Misic* (*Misic*)[27] in which the association of the medium and the message was discussed.[28] *Misic* was decided before the extended definition of a document was enacted in the amendments to the Crimes Act in 2003, but pointed out that a document was a record of information and that as such a computer programme and the medium upon which it was contained were material things which together recorded and provided information and were readily comprehended by the term document.[29]

It should be noted that *Misic* did not deal with the issue of whether a document was property, nor did it consider whether or not the information contained upon the medium constituted property. What was considered was the conceptual requirements of a document which involved an understanding of what a document did – recorded information – and how that was achieved – the association of the information (message) with the medium for the purposes of offences involving documents under the Crimes Act. What the Supreme Court appears to have done is to take the concept of digital information associated with a medium (a document) and extended that concept to extend to property.[30]

[24] At [25].
[25] At [25].
[26] At [28]–[29].
[27] *R v Misic* [2001] 3 NZLR 1 (CA).
[28] *Dixon* SC, above n 1, at [31].
[29] At [31]. See *R v Misic*, above n 27, at [34].
[30] At [31]. The emphasis seemed to be on materiality that arose from the medium/information association. The Court observed "the computer programme and the disc constituted 'material things which record and provide information' and as such were readily comprehended by the term 'document'" (at [31]).

3. *The Scope of s 249*

The scope of s 249 came under some scrutiny. The proposition was advanced by the Court of Appeal that when one obtained property by dishonestly accessing a computer system, what was comprehended was obtaining goods by a dishonest transaction – for example using false credit card details to obtain goods.[31] The Supreme Court considered that the term "property" in s 249 was wider than that and had a broader construction.[32]

The Court looked at the concept of property within the context of the definition of a computer system which included "stored data" and then went on to consider the offence contained in the provisions of s 250. That offence specifically refers to damaging, deleting, modifying or interfering with or impairing any data or software in any computer system[33] or causing data or software in a computer system to be damaged, deleted modified or otherwise interfered with or impaired.[34]

4. *Software or Data?*

It is difficult to understand why the Supreme Court followed this particular path. Although it is correct that the definition of a computer system includes stored data, there is a specific reference to data and software as the target of damage, for example, in s 250(2). Furthermore, it should be understood that s 250 deals with the *operation* of a computer system and creates an offence effectively of interfering with the *operation* of a computer system by damaging or interfering with data or software.

The offence recognises that data and software are essential for the operation of a computer system. Section 250 cannot be employed, directly or indirectly either to suggest that data and software are property. The Court incorrectly made the following comment:[35]

> Accordingly, there is no doubt that Parliament had stored data in mind when these provisions were drafted. Equally, there is no doubt that Parliament had in mind situations where stored data was copied.

With respect, this is a conclusion that cannot be reached on the basis of the line of reasoning employed. The separate use of the words "data" or "software" in the section would suggest that any implication that "stored data" was included would be redundant.[36] Furthermore, as has been noted, the use of the terms "computer system"

---

[31] *Dixon* CA, above n 2, at [38].
[32] *Dixon* SC, above n 1, at [34].
[33] Crimes Act, s 250(2)(a).
[34] Section 250(2)(b).
[35] *Dixon* SC, above n 1, at [35].
[36] "Software" is defined in the Oxford English Dictionary as: "The programs and procedures required to enable a computer to perform a specific task, as opposed to the physical components of the system" and "[t]he body of system programs, including compilers and library routines, required for the operation of a particular computer and often provided by the manufacturer, as opposed to program material provided by a user for a specific task." The program material referred to is "data", which is defined in the Oxford English Dictionary as: "The quantities, characters, or symbols on which operations are performed by computers and other automatic equipment, and which may be stored or transmitted in

in s 250 refers to operation rather than componentry although it may be conceded that the damage to data or software may have implications for the operation of a peripheral such as a pointing device or a display.

It should also be noted that s 250 targets damaging, deleting, modifying or otherwise interfering with data or software that may impair computer operation. No mention is made of copying stored data. Indeed, stored data may be copied without creating any of the problems contemplated by s 250.

The problem is that the Supreme Court relies upon this incorrect premise to discuss the circumstances that are created when stored data is received from a computer when it is copied, leaving the data intact upon the device from which it is copied.[37]

The Court speculated on which offence would be committed if stored data was copied from a target device. It excluded s 250 based on the lack of interference or impairment of the data. It noted that s 252 – which criminalises intentional unauthorised access to a computer system – targets access only. The only section which could apply was s 249:[38]

> where a person accesses a computer system without authority in order to locate, copy and then deal with valuable digital files contrary to the interests of the files' owner.

5. *Property Elements*

The Court then went on to consider some of the fundamental elements of property, noting that property as defined in the Property Law Act 2007 defined property as something that was capable of being owned, whether it was tangible or intangible.[39]

The file that Mr Dixon copied onto his USB device was, as the Court described it, a compilation of sequenced images from a CCTV system that had an economic value and were capable of being sold and had a material presence[40] – the association of medium and information that was a characteristic not of property but of a document.

6. *American Authority*

The Court then gave some consideration to American authority. In this regard, care must be taken in using United States authority because there is a different approach to the concept of information as property.[41] The approach of the Supreme Court was to draw an analogy with cases where software had been treated as tangible property.[42]

---

the form of electrical signals, records on magnetic tape or punched cards, etc." *Oxford English Dictionary* (Oxford University Press, June 2017) <http://www.oed.com>.

[37] *Dixon* SC above n 1, at [35].

[38] At [36]–[37].

[39] At [38].

[40] At [39].

[41] See David Harvey *Collisions in the Digital Paradigm: Law and Rulemaking in the Internet Age* (Hart Publishing, Oxford, 2017) at 138 et seq [Harvey *Collisions in the Digital Paradigm*] for a full discussion.

[42] *Dixon* SC, above n 1, at [40] (citing *South Central Bell Telephone v Bartelemy* 643 So 2d 1240 (Lou 1994)).

The issue of property in the context of software is a complex one and depends very much upon the circumstances of the case. For example, software falls within the definition of "goods" for the purposes of Part III of the Contract and Commercial Law Act 2017.[43] The issue of the tangibility of software code for depreciation in the context of tax provides a further and different context.[44]

7. *Electronic Conversion*

The Court also gave consideration to American authority which held that electronic records and databases had been held to be property capable of being converted,[45] referring to the case of *Thyroff v Nationwide Mutual Insurance Co* (*Thyroff*).[46] The issue in that case was whether or not there could be conversion of electronic records which were intangible. It was held that conversion was available notwithstanding intangibility on the basis that the electronic records were functionally equivalent to tangible property.[47]

8. *"Document Merger" and Conversion*

It should be noted that the problem of conversions of intangibles was addressed in the case of *Kremen v Cohen* (*Kremen*)[48] where the Court applied the theory of "document merger".

The court discussed the concept of merger of intangible rights in a tangible item such as a document. This theory developed in the American Restatement of Torts recommended:[49]

> 1. Where there is conversion of a document in which intangible rights merged, the damages include the value of such rights.
> 2. One who effectively prevents the exercise of intangible rights of the kind customarily merged in a document is subject to a liability similar to that of conversion, even though the document is itself not converted.

Kozinski J observed that courts routinely applied the tort to intangibles without inquiring whether they are merged in a document and, while it was often possible to find a document to which the intangible is connected, it was seldom one that represented the owner's property interest. The court considered that the issue of merger was minimal, requiring only some connection to a document or a tangible object.

---

[43] Part 3 of the Contract and Commercial Law Act 2017 contains the former Sale of Goods Act 1908.
[44] *Erris Promotions Ltd v Commissioner of Inland Revenue* [2004] 1 NZLR 811(HC).
[45] *Dixon* SC, above n 1, at [47].
[46] *Thyroff v Nationwide Mutual Insurance Co* 8 NY 3d 283 (NY 2007).
[47] Discussed in *Dixon* SC, above n 1, at [47]–[48]. For the problems of using the concept of "functional equivalence" as an argument to explain paradigmatically different types of information, see Harvey *Collisions in the Digital Paradigm* at 55-63.
[48] *Kremen v Cohen* 337 F 3d 1024 (9th Cir 2003). For a full discussion of *Kremen v Cohen*, see Harvey *Collisions in the Digital Paradigm* at 140 et seq.
[49] American Law Institute *Restatement (Second) of Torts* (4 Vols) § 242 (Philadelphia, American Law Institute, 1965).

Kremen involved an action for a converted domain name. The "document" or collection of documents was the electronic database that comprised the Domain Name Server. Thus *Kremen* demonstrates the analytical process that does not appear to have been present in *Thyroff* which preferred to use the suspect approach of functional equivalence.

9. *Confusing Software and Data*

In *South Central Bell Telephone v Bartelemy*[50] the issue was whether or not computer software was tangible personal property and the Court in that case discussed in some detail what software does, noting that it was a program – a set of instructions that tells a computer what to do and when stored upon a medium the machine-readable code is a physical manifestation of information in binary form.[51]

The problem that arises from this approach is conflating software – correctly described as the instructions that make a computer work – with a data file which is information – in *Dixon* the CCTV file. Software such as Microsoft Word is recorded in machine language in binary format but has quite a different function from a data file – say a Word.docx file – that requires the software to read it. The Court of Appeal had referred to a computer file as a "stored sequence of bytes." The file which constitutes the "stored sequence of bytes" which could not be distinguished from "pure information" is the visual representation that appears on a directory screen. The reality behind that visual representation is quite different.[52]

The Supreme Court deconstructed this approach by commencing with a consideration of the nature of a document. But as has been demonstrated, both in the case of *Misic* and in the definition of document in the Crimes Act the important aspect is the association of information with a medium for a particular purpose. The Supreme Court then took the definition of document and the example of a Microsoft Word document and considered it odd that a Word document would not fall under the definition of property for the purposes of s 249(1)(a) of the Crimes Act.[53]

The Court concluded, along with the Court of Appeal, that Mr Dixon's conduct fell within the ambit of s 249 and there is no doubt that it did. The Supreme Court was prepared to hold that the computer file was property and both statutory purpose and context supported that view.

It will be plain by now that the author does not unreservedly agree. There are a number of areas where *Dixon* is in error. The first is that the findings and some of the assumptions used by the Supreme Court do not accord with technological reality. Secondly, the decision brings a significant element of inconsistency into the law. Thirdly, the decision and the holdings in *Dixon* are procedurally unsound. Finally, the

[50] *South Central Bell Telephone v Bartelemy*, above n 42.
[51] At 1243. It should be observed that there is not complete consensus among US courts that software amounts to tangible property. See Ken Moon "The Nature of Computer Programs: Tangible? Goods? Personal Property? Intellectual Property?" (2009) 31 EIPR 396 at 399.
[52] As discussed below.
[53] *Dixon* SC, above n 1, at [47].

decision will lead and has led, to consequences that were unintended by the Supreme Court and introduce wider scope to "digital crime" than was intended by the Crimes Act.

V. Critiquing Dixon

A. Technological Reality[54]

Throughout the decision, the Supreme Court seems to assume that a digital data file is a coherent whole. The difficulty started in the argument that was advanced by counsel for the Crown, who argued that a USB stick is equivalent to a roll of film and a computer file to a paper file.[55] The Supreme Court seems to have adopted that theory of the nature of digital data in referring to the digital files as a "compilation of sequenced images from the bar's CCTV system"[56] and a "stored sequence of bytes".[57]

1. *Incorrect Comparisons*

The problem with the analogies advanced by the Crown is that they use comparators that involve fundamentally different ways of retaining information or data. A roll of film is a celluloid medium which, as a result of treatment with chemicals, is capable of storing images. A paper file consists of a medium – paper – upon which information is written or printed. Both media contain information in a complete, sequential, linear and coherent form.

A digital file does not do that. The bytes that make up the file are not in a sequence. They are not in a compilation. Depending upon the medium upon which the bytes are stored, they may be arranged in fundamentally different ways.

2. *Data Storage*

None of this is apparent to the computer or device user. This is because of the way in which file and directory information is presented on a screen by the particular operating system. Generally the information is presented by means of a directory and file structure.[58] The term "directory" refers to the way a structured list of files and folders is stored on a computer. The hierarchical file system that is used in computing is represented in the familiar graphical interface as a collection of folders and files. But this graphical representation in no way reflects the reality of how digital data – be it software programs or data – is stored on a medium such as a hard drive. It is helpful for the user for the purposes of locating, executing or accessing a program or data but really it is the information that is contained within the directory sector of the medium. This sector contains all the information about where the various bytes that make up the file or program may be located throughout the medium.

---

[54] This issue received a similar treatment to that which follows in Harvey *Collisions in the Digital Paradigm* at 135 et seq.
[55] *Dixon* SC, above n 1, at 682.
[56] At [39].
[57] At [45].
[58] Although Unix treats a directory as a type of file.

To add another layer of complexity to the issue, it should be noted that data used by a computer may be located in primary storage[59] which is directly accessible by the computer processor. Data in primary storage is volatile, unlike data in secondary storage which is not directly accessible by the processor such as hard drives, USB drives or other external storage devices.[60]

It immediately becomes clear that it is unwise to make generalised assumptions about the nature of computer data when there are a number of variables that have to be considered.

3. *Common Terms*

Many of the terms that we use and the assumptions we adopt when dealing with digital data arise from our unfamiliarity with a paradigmatically different way of dealing with information. We use of familiar terms and metaphors to help us feel more comfortable in the new digital space. Thus we use the term "documents" because on a screen the information has the same visual appearance as print on paper. We "turn" the pages on our Kindles or eReaders and "put" them in files or folders. Email also mimics the traditional hard copy letter which we "write" rather than type.[61]

These terms and assumptions, and the way that the information is presented to us on a screen can create the misleading impression that the electronic file exists somewhere on the computer as a single, complete whole and maintains its structural integrity even when the computer is turned off in the same way that a paper document or a film continue to exist when put into a file folder or a canister.[62]

4. *Hardware and Software Dependency*

Data in electronic format is dependent upon hardware and software. This was the subject of an oblique reference by the Supreme Court when it observed that files "have a physical presence, albeit one that cannot be detected with the unaided senses".[63] However, the Court did not go on to examine the way in which the file is stored and accessed on a device.

The data contained upon a medium such as a hard drive requires an interpreter to render it into human readable format. The interpreter is a combination of hardware and software. Unlike the paper document, the reader cannot create or manipulate

[59] Such as data stored in the random access memory (RAM) or the read only memory (ROM).
[60] George RS Weir and Stephen Mason "The sources of electronic evidence" in S Mason (ed) *Electronic Evidence* (4th ed) (University of London, London, 2017) at 4 (available in electronic format under a Creative Commons Licence at <http://humanities-digital-library.sas.ac.uk/index.php/hdl/catalog/book/electronicevidence>) [Mason *Electronic Evidence*].
[61] Burkhard Schafer and Stephen Mason "The Characteristics of Electronic Evidence" in Mason *Electronic Evidence*, above n 60, at 20.
[62] At 20.
[63] *Dixon* SC, above n 1, at [25].

electronic data into readable form without the proper hardware in the form of computers.[64]

There is 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. Because of the way in which electronic storage media are constructed it is almost impossible for a complete file of electronic information to be stored in consecutive sectors of a medium. An electronic file is better understood as a *process* by which otherwise unintelligible pieces of data are distributed over a storage medium, are assembled, processed and rendered legible for a human user. In this respect, the "information" or "file" as a single entity is in fact nowhere. It does not exist independently from the *process* that recreates it every time a user opens it on a screen.[65]

Computers are useless unless the associated software is loaded onto the hardware. Both hardware and software produce additional digital material that includes, but is not limited to, information such as metadata and computer logs that may be relevant to any given file or document in electronic format.

This involvement of technology and machinery makes electronic information paradigmatically different from traditional information where the message and the medium are one. It is this mediation of a set of technologies that enables data in electronic format – in its basic form, positive and negative electromagnetic impulses recorded upon a medium – to be rendered into human readable form. This gives rise to other differentiation issues such as whether or not there is a definitive representation of a particular source digital object. Much will depend, for example, upon the word processing programme or internet browser used.

The necessity for this form of mediation for information acquisition and communication explains the apparent fascination that people have with devices such as smart phones and tablets. These devices are necessary to "decode" information and allow for its comprehension and communication.

Thus, the subtext to the description of the electronically stored footage which seems to suggest a coherence of data similar to that contained on a strip of film cannot be sustained. The "electronically stored footage" is meaningless as data without a form of technological mediation to assemble and present the data in coherent form. The Court made reference to the problem of trying to draw an analogy between computer data and non-digital information or data and referred to the example of the Word document.[66] This is part of an example of the nature of "information as process" that I have described above. Nevertheless, there is an inference of coherence of information in a computer file that is not present in the electronic medium – references to "sequence of bytes" are probably correct once the assembly of data prior to presentation on a screen has taken place - but the reality is that throughout the

[64] Burkhard Schafer and Stephen Mason, "The Characteristics of Electronic Evidence" in Mason *Electronic Evidence*, above n 60, at 21–22.
[65] At 22.
[66] *Dixon* SC, above n 1, at [31] and [46].

process of information display on a screen 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.

Underlying the approach of the Supreme Court is an assumption of coherence of digital content – be it described as data or information – sequentiality and identifiability independent of the machine. This assumption is incorrect

B. Inconsistency

The Supreme Court was considering the nature of a digital file as property for the purposes of s 249(1)(a) of the Crimes Act. Thus a digital file as property was limited to that section.

However, the failure of the Court to address the "orthodox view" that there is no property in information creates confusion and inconsistency in the law. For example, the decision of *Oxford v Moss,*[67] which held that information could not be property for the purposes of a charge of theft, still remains. The Canadian case of *Stewart v R*[68] dealt with the issue of whether confidential information could be property and the subject of theft. In that case, confidential information was held to be intangible and did not qualify as "anything" under the Canadian statute and was not capable of conversion. That case might still be good authority because of the way in which the Supreme Court limited the definition of a digital file as property to charges under s 249.

The issue of the susceptibility of digital data to remedies such as a possessory lien was dealt with in the case of *Your Response Limited v Data Team Business Media Limited*,[69] where it was held that digital data could not be the subject of a possessory lien, referring to *OBG v Allen*,[70] which held that wrongful interference with contractual rights could not constitute the tort of conversion because the tort applied to chattels and not to choses in action.

As matters stood following the Court of Appeal decisions in *Dixon* and *Watchorn,* there was overall consistency in the approach of the law to the issue of property in information and digital data as a form of information. The decision of the Supreme Court muddies the water, holding that digital data is property for a particular section of the Crimes Act, but not for others. This inconsistent approach to property and digital data makes the law unclear and uncertain. The answer to the question "is there property in a digital file?" is "it depends".

[67] *Oxford v Moss* (1979) 68 Cr App R 183 (QB).
[68] *Stewart v R* [1988] 1 SCR 963.
[69] *Your Response Limited v Data Team Business Media Limited* [2014] EWCA Civ 281.
[70] *OBG v Allen* [2007] UKHL 21, [2008] 1 AC 1.

C. Procedural Unsoundness

There were aspects of the way in which *Dixon* was heard which cause concern. The problem was partly of Mr Dixon's own making, in that he dispensed with his counsel before the appeal. Consequently, he was not equipped to argue the issue of the nature of property or provide an effective argument to those advanced on the part of the respondent. The report of the case indicated a detailed argument was advanced on behalf of the Crown,[71] addressing issues of some significance for the development of the law.

Given that the decision seems to adopt many of the arguments advanced by the Crown, this commentator is of the view that on a matter as important as a consideration of the nature of property in a digital file, the Court should have appointed *amicus curiae* to provide a measure of balance in the argument.

The second area of concern lies in the way in which the Court took it upon itself to deal with the case of *Watchorn.*[72] The Court observed that it did not agree that the digital files obtained by the defendant in that case were not property. Mr Watchorn had been convicted at trial on three charges of breaches of s 249(1)(a) but that conviction was set aside and, as has been noted, no alternative charge was substituted.

The Supreme Court observed that it considered that the files were property and that, because the other elements of dishonesty and absence of claim of right were upheld by the Court of Appeal, the conviction entered in the District Court was properly entered.

No opportunity was afforded Mr Watchorn or his counsel to argue this issue, and it appears that the Court embarked upon this discussion to make sure that there was no conflict between its holding in *Dixon* and the decision in *Watchorn*. There should have been an opportunity afforded Mr Watchorn or his counsel to be heard, especially in light of the gratuitous observation that Mr Watchorn had been properly convicted, even although that conviction had been overturned.

VI. Unintended Consequences

Even though the decision of the Supreme Court is unsatisfactory for the reasons outlined, the limitation of the definition of property in a digital file for the purposes of s 249(1)(a) should have prevented a degree of "creep" in extending the scope of the definition. That has not proven to be the case and the possible "law of unintended consequences" could well come into play.

[71] *Dixon* SC, above n 1, at 680–682.
[72] At [54].

A. Expanding Dixon – Ortmann v United States

The decision in *Ortmann v United States*[73] was an appeal against the decision of Judge Dawson approving the eligibility for the extradition of Kim Dotcom and his associates.

Briefly put it was necessary for the Court to consider the indictment that had been proferred in the United States and the charges which the accused appellants were to face in that country and determine whether or not they amounted to extraditable offences for the purposes of the Extradition Act 1999.

Gilbert J considered a number of different offences under New Zealand law which were "pathways" to the counts in the indictment alleging conspiracy to commit copyright infringement.[74] In doing so, the Court considered the applicability of certain offences in the Crimes Act that did not directly address copyright infringement but where the behaviour might include that activity.

A number of pathway offences were considered. One, under s 228 of the Crimes Act, involved the use of a document.[75] The definition of a document included digital material and was available. Another pathway was available pursuant to s 249(1)(a) of the Crimes Act.[76] On the basis of the holding by the Supreme Court in *Dixon* the digital files amounted to property as an element of that offence.

Gilbert J also considered the availability of s 240 of the Crimes Act as a pathway offence.[77] That section creates the offence of obtaining or causing loss by deception. There are four circumstances in which the offence may occur, all of them requiring elements of deception on the part of the perpetrator together with an absence of claim of right.

It was conceded that the element of deception could be made out as could the element of obtaining.

For the offence to be complete, property had to be obtained. Gilbert J held that the copyright protected films in digital file format were property and cited *Dixon*[78] as his authority.[79]

In this commentator's respectful view Gilbert J read *Dixon* more widely than was available to him. As has been noted *Dixon* centred around whether or not a digital file was property for the purposes of s 249 of the Crimes Act. The scope of the holding that a digital file is property is limited to the provisions of s 249 of the Crimes Act.[80] The Supreme Court held thus, and to expand the scope of the finding to include digital

---

[73] *Ortmann v United States* [2017] NZHC 189 [*Ortmann v US*].
[74] At [57]–[238].
[75] At [138]–[160] and [220]–[222].
[76] At [161]–[168] and [226]–[230].
[77] At [223]–[225]
[78] *Dixon* SC, above n 1.
[79] *Ortmann v US*, above n 73, at [225].
[80] *Dixon* SC, above n 1, at [50]–[51]

files as property for offences other than under s 249 is, in my respectful view, a misinterpretation of *Dixon.*

A consequence of this is that Gilbert J has opened the door to broaden the scope of the concept of digital files as property beyond the limited approach adopted by the Supreme Court.

B. Further consequences: Crimes Act 1961, s 246 (receiving)

One example may be found where the person who accesses a computer system dishonestly and without claim of right, and obtains a digital file containing embarrassing or damaging information. That information, if published, could have significant consequences. The "hacker", for so he is, puts the information onto a USB stick. The information is delivered to a third party. There are no criminal implications in the hacker giving the third party the USB stick. Property in the USB stick itself and as a medium is validly transferred. What of the digital file on the USB stick? Assume that the third party is aware that the file was obtained dishonestly and by unauthorised access to a computer system.

The question which may need to be asked and answered is whether or not the receipt of the digital file on the USB stick would be sufficient to constitute the offence of receiving by the third party. If the digital file is property distinct from the USB medium, the answer would be in the affirmative.

C. Criminalising intellectual property infringement

Under the law as it stands, copying digital material that is subject to copyright exposes the copier to possible proceedings for infringement[81]. Because a digital file may amount to property under Gilbert J's extension of the holding in *Dixon* it would be open to copyright owners to deploy the provisions of s 249(1)(a) to deal with what would otherwise be copyright infringement in the digital space but which may amount to criminal behaviour.

VII. CONCLUSION

In *Stevens v Kabushiki Kaisha Sony Computer Entertainment Ltd*[82] at issue was the question of the interpretation of a provision of Australian copyright legislation. The High Court cautioned against courts getting involved in making policy decisions about legislation which was properly the bailiwick of Parliament. The Court observed:[83]

> The Parliament having chosen such an elaborate and specific definition for the key provision of the legislative scheme, a court should pause before stretching the highly specific language in order to overcome a supposed practical problem.

[81] Copyright Act 1994, s 120 et seq.
[82] *Stevens v Kabushiki Kaisha Sony Computer Entertainment Ltd* [2005] HCA 58; (2005) 224 CLR 193; (2005) 221 ALR 448.
[83] At [204].

The Supreme Court in *Dixon* observed in its discussion of the legislative history that Parliament had stepped away from a definition of property that would have included a digital file. That in itself should have sent a message. The Court seems to have decided to embark upon an exercise in expediency and judicial legislation which properly should have been left to Parliament. Whether the unintended consequences and extensions of the decision will eventuate remains to be seen.