1 of 1 DOCUMENT: New Zealand Law Journal/2016/No 4 -- May 2016/Using the criminal law computer misuse provisions to protect confidential information

[2016] NZLJ 128

Using the criminal law computer misuse provisions to protect confidential information

Anna Kingsbury, University of Waikato, looks at recent cases under s 249 of the Crimes Act

INTRODUCTION

This article is about the criminal law provisions relating to crimes involving computers, and the risks these provisions may pose to people dealing with confidential information in the nature of a trade secret, as illustrated by recent cases.

There is a growing international trend toward use of the criminal law to protect confidential information and trade secrets. A growing number of jurisdictions have criminal provisions applying in some form to the taking of trade secrets. United States law has included such criminal provisions for some years. New Zealand law has also had provisions since 2003, and requirements for such provisions are being included in trade agreements such as the Trans-Pacific Partnership Agreement (TPPA). The primary justification for criminalisation is generally concern about foreign hackers, but inevitably employees and ex-employees are among the likely defendants.

There has not yet been a lot of case law involving the taking of confidential information under the New Zealand provisions, but there have been two significant recent cases. This article reviews the recent New Zealand cases and considers the implications for employees and others dealing with confidential information. It is arguable that the availability of the criminal law in these cases creates excessive risks for individual employees and more broadly for employee mobility and the sharing of information, perhaps most troublingly in knowledge-based industries.

CRIMINAL LAW PROTECTION OF CONFIDENTIAL INFORMATION

The common law countries have traditionally used the civil law to provide legal protection for confidential information, including trade secrets. New Zealand law has followed English law and provided legal protection for confidential information through the action for breach of confidence. In recent years, however, concerns about digital technologies and the increased possibilities for taking of information these technologies provide has led to the introduction of criminal offences for computer misuse, including a new offence for the taking of trade secrets. Section 230 of the Crimes Act 1961 as amended in 2003 provides for an offence of taking, obtaining or copying trade secrets. The penalty on conviction is imprisonment for up to 5 years.

In enacting the provision, legislators in part reacted to concerns about computer hacking, and to concerns about perceived threats from foreigners wishing to steal New Zealand government information and trade secrets held in the private sector. New Zealand is one of few comparable countries to have a criminal offence for the taking of trade secrets as well as the possibility of civil action for breach of confidence.

In addition to s 230, ss 248 to 254 of the Crimes Act set out crimes involving computers, all carrying a prison term. These include an offence of damaging or interfering with a computer system (s 250), an offence of accessing a computer system without authorisation, (s 252) and an offence of accessing a computer system for a dishonest purpose (s 249).

Although New Zealand law includes (in s 230) an express provision providing for an offence of taking, obtaining or copying a trade secret, New Zealand has not seen criminal prosecutions under this section. However, cases involving the taking of information have been prosecuted under the other computer misuse provisions, particularly s 249(1) which prohibits accessing a computer system for a dishonest purpose. Section 249 provides for up to 7 years imprisonment for directly or indirectly accessing any computer system and, dishonestly or by deception, and without claim of right, obtaining any property, privilege, service, pecuniary advantage, benefit, or valuable consideration; or causing loss to any other person. Under this provision, there is no need to show that a document has been taken, obtained or copied. There is no need to establish that any information taken meets the definition of a "trade secret" as in s 230. In addition, s 249(2)

prohibits directly or indirectly accessing any computer system *having the intent* to do any of the acts in s 249(1), and is directed at attempts.

SECTION 249 CASES

Watchorn v R [2014] NZCA 493

Section 249 was used in a trade secret type situation in the 2014 Court of Appeal decision in *Watchorn v R*. The case involved James Watchorn, a production/facility manager who had been employed by TAG Oil (NZ) Ltd, an oil and gas exploration and mining company. He was accused of downloading information from the TAG computer system. He had downloaded the data in anticipation of moving to another employer, but he had not misused the data. The case between the parties was heard by the Employment Relations Authority which awarded TAG special damages of $65,567 and penalties of $12,000 (*TAG Oil (NZ) Ltd v Watchorn* [2014] NZERA Wellington 58 5393742).

In a subsequent criminal case, Mr Watchorn was convicted of accessing a computer system and thereby dishonestly and without claim of right obtaining property, and was sentenced to two and a half years imprisonment. The decision was appealed, and on appeal the main issue was whether the data was in fact "property". It was argued that he had instead obtained a "benefit". The Court of Appeal held that it was not property, quashed the convictions and did not order a retrial, as he had already served a sentence of five weeks prison time. The Court of Appeal also said that the prison sentence was excessive.

On the facts, Mr Watchorn had taken data to which he was not entitled, and this had been dealt with as an employment matter. Although the case was on the computer misuse provision, it does raise issues as to the role of the criminal law in cases in which trade secrets are taken. This was not a case of foreign economic espionage in any sense. It was an employee moving to a new employer. The defendant was clearly at fault, having downloaded data that he should not have downloaded and breached his obligation to his employer and his employment agreement, although he had not used the information to compete with his employer. The case was heard by the Employment Relations Authority, and remedies and penalties were ordered. It is difficult to see the need for intervention of the criminal law in what was at heart an employment relationship dispute.

Dixon v R [2015] NZSC 147

A second, and more well-known, recent New Zealand case raising similar issues is the October 2015 Supreme Court decision in *Dixon v R*. Mr Dixon worked for a company providing security services to a Queenstown bar. Mr Dixon obtained closed circuit television (CCTV) footage showing a member of the English rugby team socialising and leaving the bar. He tried, unsuccessfully, to sell the footage to the media, and eventually posted it on YouTube. The District Court judge said that he had posted the footage on YouTube out of spite, and to prevent anyone else from making money out of it (*R v Dixon* DC Invercargill CRI-2011-059-1122, 2 August 2013 (Sentencing), at [11], referred to in *Dixon v R* [2015] NZSC 147 at [15]).

The *Dixon* case was not a case involving the direct taking of information by an employee, as he worked for a security company providing services to the bar. The company that operated the bar had installed the CCTV system. Mr Dixon obtained the CCTV footage from a receptionist at the bar. The receptionist transferred the CCTV files, on Mr Dixon's request, to a desktop computer in the reception area, and Mr Dixon transferred the files from the desktop computer to a personal USB stick. The company operating the bar asked Mr Dixon to return the footage. Despite the absence of a direct employment relationship, it is nevertheless difficult to identify on the facts why this was a criminal rather than a civil matter to be resolved between the parties. The civil action for breach of confidence would have been an available avenue. The action for breach of confidence protects confidential information because of its status as confidential; there is no need to establish the existence of a property right.

Mr Dixon was nevertheless convicted by a jury in the District Court of the offence of accessing a computer system for a dishonest purpose and obtaining property under s 249(1)(a) of the Crimes Act 1961. Mr Dixon was sentenced to four months community detention and 300 hours of community work (see *R v Dixon* DC Invercargill CRI-2011-059-1122, 18 April 2013 (Summing Up) and *R v Dixon* (Sentencing) (above)). On appeal to the Court of Appeal (*Dixon v R* [2014] NZCA 329, [2014] 3 NZLR 504) the conviction was quashed on the grounds that the digital footage was not "property" for the purposes of s 249(1)(a), but substituted a conviction for obtaining a "benefit" under the same section, and the sentence remained the same. In the Supreme Court a central issue was whether the Court of Appeal was correct in holding that the CCTV files were not property, and whether Mr Dixon had obtained "property" or a "benefit" for the

purposes of s 249. The Supreme Court held, controversially, that digital files could be distinguished from pure information, and that digital files could be property for the purposes of s 249(1)(a). Mr Dixon had therefore obtained "property" rather than a "benefit". The Supreme Court was clear that it was not reconsidering the orthodox view that "pure information" was not property.

The Supreme Court also discussed the *Watchorn* case in its judgment in *Dixon*. In *Watchorn* the Court of Appeal had accepted the Crown's concession, in light of the Court of Appeal decision in *Dixon*, that data obtained from a computer is not "property". The Supreme Court said that, on the basis of its analysis in *Dixon*, the digital files obtained by Mr Watchorn were "property" for the purposes of s 249(1)(a), and Mr Watchorn was properly convicted on that basis.

The Supreme Court's decision that digital files can be property does raise some difficult questions. The Supreme Court was clear that that it was taking the view that digital files could be distinguished from pure information, and that it was not reconsidering the orthodox view that "pure information" was not property. In this, it agreed with the Court of Appeal. The Court of Appeal in *Dixon* had considered this issue, and referred to the case of *Oxford v Moss* (1979) 68 Cr App R 183 in which the taking of information was not theft because the information was not property. The Court of Appeal also referred to two New Zealand cases in which *Oxford v Moss* had been followed (*Money Managers Ltd v Foxbridge Trading Ltd* HC Hamilton CP67/93, 15 December 1993 and *Taxation Review Authority 25* [1997] TRNZ 129) and to the prevailing view in the civil law of breach of confidence that confidential information is not property (referring to *Hunt v A* [2007] NZCA 332, [2008] 1 NZLR 368).

The Supreme Court was not therefore questioning the established position that information is not property. Confidential information is protected by the civil law because it is confidential, not because it is property. Generally, when confidential information is described as "intellectual property" this is a metaphorical usage of the term "property". The authors of *Gurry on Breach of Confidence* (T Aplin, L Bently, P Johnson and S Malynicz, *Gurry on Breach of Confidence* (2ed, 2012) 316), for example, have said that:

> Our view is that there is no such thing as ownership or co-ownership of confidential information because information does not give rise to property rights that may be owned. Rather, the language of 'ownership' (as with that of 'property'), if it is used at all, tends to be used in a loose, metaphorical sense to indicate that a person has an interest in protecting the confidential information.

The Supreme Court was rightly in agreement with the Court of Appeal that information is not property. The Court of Appeal noted the strong policy reasons militating against recognition of information as property, particularly in relation to the public interest in the free flow of information and freedom of speech. The Court of Appeal also noted that Parliament had amended the definition of property in s 2 of the Crimes Act at the time it created the new computer-related offences, and had not included a reference to computer-stored data.

The Supreme Court however differed with the Court of Appeal on the issue as to whether a digital file was distinguishable from confidential information. The Court of Appeal considered whether a digital file might be viewed as being the medium in which information is contained. The Court said that it was arguable that a digital file did have a physical existence in a way that information did not. However the Court of Appeal took the view that electronic footage stored on a computer was indistinguishable in principle from pure information, and that it was problematic to treat computer data as being analogous to information recorded in physical form. The Court said that a computer file was essentially just a stored sequence of bytes available to a computer program or operating system, and could not meaningfully be distinguished from pure information. The Court of Appeal therefore held that information, including digital data, was not property for the purposes of s 2 of the Crimes Act. The Court said that the reference to property in s 249 was aimed at situations such as the taking of credit card details in order to unlawfully obtain goods. The Court also said that s 230, criminalising the taking of trade secrets, would be unnecessary if confidential information was property.

The Supreme Court disagreed with the Court of Appeal. The Supreme Court arguably mischaracterised the reasoning of the Court of Appeal, saying that the Court of Appeal held that the digital files were "pure information" and therefore not property. The Court of Appeal reasoning was actually a little more complex, and concluded that the electronic footage was "indistinguishable in principle from pure information". Nevertheless, the Supreme Court disagreed, holding that the digital files were property and not simply information. The digital files could be identified, had a value, were capable of being transferred to others, and had a physical presence although they could not be detected by the unaided senses. It is, of course, arguable that information has many of the same characteristics but is still not property -- it can be identified, it has value and is capable of being transferred. The distinction here is perhaps better made on the basis of physical presence. The Supreme Court also said that the fundamental characteristic of property was that it was something capa-

ble of being owned and transferred. This is arguably circular reasoning -- it is only capable of being owned, after all, if it is property.

The Supreme Court drew support from the definition of property proposed at the time the computer offences were created, which would have included "all things", and the Court did not think that the fact the definition was not enacted was material. The Court also took account of the Crimes Act, s 217(c) definition of "document", which included material held in electronic form. The Court of Appeal had not regarded this as relevant to the question of whether digital files were property, as the word "document" did not appear in the definition of "property". It is difficult to see why the Court of Appeal was wrong on this point. The Supreme Court also considered that in the context of the other computer offences it was appropriate to find that the digital files were property in order to cover the conduct at issue. This was despite the potential for the conduct to be caught by "benefit".

The Supreme Court noted that some United States courts had treated electronic records and databases as property capable of being converted, although the position was different in England. United States courts also treated software as property, and the Supreme Court said that there seemed no reason to treat data files differently. The Court did not elaborate on this point, which on its face seems potentially problematic, as there are significant difference between a digital file and software.

The Supreme Court held that what Mr Dixon took was property. The court also doubted whether he had obtained a "benefit" on the facts. In the event, Mr Dixon's original conviction was reinstated and he was required to complete his sentence.

The Supreme Court decision in *Dixon* therefore opens up the possibilities of criminal prosecution, and a jail term, for the taking of property where what is taken is a digital file, and where the other elements of the offence are met. The other elements include the showing that the computer system was accessed directly or indirectly, and that the act was done dishonestly or by deception and without claim of right. In relation to accessing a computer system, there are two relevant definitions in the statute. Section 248 provides that "access, in relation to any computer system means instruct, communicate with, store data in, receive data from, or otherwise make use of any of the resources of the computer system". The section also defines "computer system" although there is no definition of "computer". In Mr Dixon's case, there was no doubt that he had accessed a computer system within the meaning of s 249(1)(a).

These New Zealand cases were not brought under the criminal trade secret provision, but they demonstrate that cases where trade secrets have been acquired from a computer system can be prosecuted under s 249, irrespective of financial advantage to the person, commonly an employee or similar, who is obtaining the information. It is arguable that in many cases it will be significantly easier to bring trade secret type cases under s 249 than under s 230. Under s 249 there is no need to prove that the digital file or data taken is a trade secret as defined. Section 230(2) defines trade secret to mean any information that:

(a) is, or has the potential to be, used industrially or commercially; and
(b) is not generally available in industrial or commercial use; and
(c) has economic value or potential economic value to the possessor of the information; and
(d) is the subject of all reasonable efforts to preserve its secrecy.

Section 230(1) also requires that the defendant know that the document, model or other depiction taken contains or embodies a trade secret, and requires intent to obtain pecuniary advantage or to cause loss to any other person. These are not required for s 249, so that the s 249 dishonesty element becomes important.

CONCLUSION

These cases involve the taking of confidential information, and have been prosecuted under s 249 as accessing a computer system for a dishonest purpose. They evidence the way in which the section can be used in a trade secret context, and that it is in fact easier in many cases to bring an action under s 249 rather than under s 230 which is designed for trade secret protection. This is particularly the case once digital files are regarded as property for the purpose of the section.

The cases suggest that employees, ex-employees and others are likely to be subject to such enforcement action, no doubt in many cases with justification. However, there is also cause for disquiet that, especially in knowledge-based industries, there is a risk that enforcement may be either excessive, or based on an inexpert understanding of the nature of the information allegedly taken. Since in contemporary workplaces most cases of taking of trade secrets will involve

accessing a computer, the scope for trade secret type cases to be prosecuted under the computer misuse sections is substantial, and a significant risk for employees and others over and above liability under the civil law action for breach of confidence.[ ]