E.I.P.R. 2016, 38(4), 237-245

European Intellectual Property Review
2016

The Trans-Pacific Partnership Agreement and the protection of commercial confidential information and trade secrets in New Zealand law

Dr Anna **Kingsbury** [1]

© 2016 Sweet & Maxwell and its Contributors

Subject: Intellectual property
Other Related Subject: Criminal law. International trade.

Keywords: Criminal liability; New Zealand; Plurilateral trade agreements; Trade secrets;

Legislation:

Trans-Pacific Partnership Agreement 2015art.18

TRIPS Agreement

Crimes Act 1961 (New Zealand)s.230, s.249, s.252

***237** *A number of initiatives are in progress internationally to strengthen and harmonise trade secrets law, and trade secrecy provisions can be expected in new trade agreements. This article analyses the trade secrecy provisions in the recently concluded Trans-Pacific Partnership Agreement (TPPA) to which New Zealand is a party, and the potential impact these provisions will have on New Zealand law.*

Introduction

After many years in which trade secrets law received relatively little attention internationally, we are now seeing a flurry of activity aimed at harmonising trade secret protection, combined with efforts to increase the level of protection provided by law. Internationally, there have been a number of initiatives to increase trade secret protection, driven by concerns about economic espionage, especially foreign economic espionage. [1] This article is about one such initiative, the trade secret provisions in the recently concluded Trans-Pacific Partnership Agreement (TPPA) to which New Zealand is a party, and the impact these provisions will have on New Zealand law.

The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) contains minimum standards for trade secret protection, [2] but there is considerable international variation in the legal mechanisms for providing that protection, and variation in the levels of protection. In the US, the Uniform Trade Secrets Act provides one approach that is used in most states. [3] The US also enacted the Economic Espionage Act in 1996, [4] providing a federal criminal law protecting trade secrets, [5] and further legislation is proposed, adding a private federal cause of action under the Economic Espionage Act. [6] In Europe, laws on trade secrets vary considerably across Member States. In 2013 the European Commission proposed a new Directive harmonising the civil law protecting trade secrets, and the European Parliament is currently considering resulting legislation. [7] The European harmonisation initiative applies only

to the civil action and does not require criminal law protection of trade secrets. Europe and the US are negotiating a Transatlantic Trade and Investment Partnership ***238** Agreement (TTIP) which is expected to contain provisions on trade secret protection, and once passed the new Directive will be the European benchmark in negotiations with the US.[8] The TPPA contains provisions requiring a higher level of protection for trade secrets than that required under TRIPS, and we can expect other agreements, such as the TTIP, to also raise the level of protection required.

This article reviews the policy objectives underlying the legal protection of confidential commercial information and trade secrets. It details the trade secret provisions in the TPPA and the implications for protection in New Zealand law. It concludes that New Zealand law does not currently comply with the TPPA trade secrets provisions, and that new legislation is likely to be required. New Zealand law-makers will have considerable flexibility as to the exact form such legislative reform will take, and it is argued that it is in the interests of New Zealand to create a coherent but not over-protective legislative regime, and a regime that does not unduly inhibit employee mobility.

Trade secrets protection—policy objectives

Businesses, including small and medium-sized enterprises, develop information which they wish to keep confidential for commercial advantage. This may be information that is kept confidential in the lead-up to a patent application, or may be information that is not patentable or relates to an invention that they have chosen not to patent. Information may relate to manufacturing processes, recipes and formulae, or business information about customers and clients. A business may seek to protect the information in the short term or in the longer term. Protection is against misappropriation, either by outsiders, generally competitors, or by people such as potential joint venture partners or employees to whom the information has been given in confidence.

The conventional justifications for laws protecting confidential commercial information are economic.[9] The ability to protect such confidential information provides an incentive to invest in research and development, and therefore promotes innovation by preventing free-riding by competitors. Trade secret protection is therefore one element in innovation policy. There are, however, competing public interests involved in the policy underpinning trade secret protection. There is a need to protect competition, and to avoid over-protection so as to stifle competition and follow-on innovation. Reverse-engineering of products on the open market is generally permitted in order to facilitate competition and further innovation.[10] Interaction with patent policy is also an important consideration; the patent system offers protection for inventions for a limited time in exchange for disclosure in the public interest. Excessive protection of trade secrets will be an incentive to maintain secrecy in preference to disclosure through patenting, and trade secret law offers the potential for protection for an unlimited term if secrecy is maintained.

Trade secret law should not be so protective that it interferes with employee mobility. Staff working for one company must be free to move to a competitor and use the skills and knowledge that they have a legitimate claim to use. Stifling employee mobility has been demonstrated to have negative effects on competition and innovation, and also can potentially lead to a "brain drain" effect, where employees move to other jurisdictions to avoid liability.[11] There is also an important human rights dimension here. Employees have a right to work in their chosen field, and this right should not be unduly limited.[12]

Additional considerations in the design of trade secrets law are the need to protect disclosures in the public interest, for example for reasons of public health and safety, consumer protection, or in situations of whistle-blowing. The protection of the freedom of expression right and journalistic freedom to receive and publish information are also important values. These issues have all been significant in current debates about the proposal to harmonise European civil law on trade secrets.[13]

There is a need to create a coherent regime that protects trade secrets sufficiently to promote innovation, but not to over-protect so as to limit competition and employee mobility and thereby limit innovation. Freedom of expression, rights to information and whistle-blower protection are important. There is little agreement internationally about whether protection should be civil only or whether civil and criminal protection should be ***239** provided for. [14] There is also little agreement on the design of any criminal offence, including on exactly which acts are to be prohibited, and whether there is a need for a specific intent element. The trade secrecy provision in the TPPA is therefore important as an indication of the direction such agreements may take. The TPPA requirement for protection requires a significantly higher level of protection than that required by the TRIPS Agreement, and importantly it requires criminal law measures, although with some flexibility as to the exact scope of those measures.

Trade secrets provisions in the TPPA and New Zealand law

The Trans-Pacific Partnership Agreement (TPPA) is a free trade agreement between 12 Pacific-Rim countries: New Zealand, Australia, Brunei Darussalam, Canada, Chile, Japan, Malaysia, Mexico, Peru, Singapore, the US and Vietnam. [15] The conclusion of negotiations was announced on 5 October 2105, and agreement is to be followed by domestic processes to put the agreement in place. [16] The Agreement contains detailed provisions in the chapter on intellectual property law, including provisions in relation to trade secrets applying to both the civil law and the criminal law. [17]

The civil law

Article 18(78)(1) of the TPPA sets out a requirement for protection of trade secrets which covers the civil law. It provides that

"each Party shall ensure that persons have the legal means to prevent trade secrets lawfully in their control from being disclosed to, acquired by, or used by others (including state-owned enterprises) without their consent in a manner contrary to honest commercial practices".

This text is similar to, but not identical to, the text in art.39(2) of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement). [18] Article 39(2) provides that:

"Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices."

The language in the TPPA is slightly stronger in stating that parties "*shall ensure* that natural and legal persons *have the legal means*" as compared with the language in the TRIPS Agreement, in which the requirement is that "natural and legal persons *shall have the possibility*".

There is a limitation to the performance of the prohibited acts of disclosure, acquisition or use "in a manner contrary to honest commercial practices". In this context, the agreement uses substantially the same wording as that used in the TRIPS Agreement. [19] The text of the TRIPS Agreement provides that

"'a manner contrary to honest commercial practices' shall mean at least practices such as breach of contract, breach of confidence and inducement to breach, and includes the acquisition of undisclosed information by third parties who knew, or were grossly negligent in failing to know, that such practices were involved in the acquisition".

The definition of "trade secret" in the TPPA is also an echo of the definition in the TRIPS Agreement. The TPPA provision defines "trade secrets" as encompassing, "at a minimum, undisclosed information as provided for in Article 39.2 of the TRIPS Agreement". Article 39(2) of the TRIPS Agreement applies to information so long as such information [20]:

(a)
"is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;

(b)
has commercial value because it is secret; and

(c)
has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret. ***240** "

The TPPA and pre-existing TRIPS requirements are therefore similar in relation to the private law action. The TPPA provision in art.18(78) appears to have been relatively uncontroversial in negotiations, although there was some concern raised in relation to the inclusion of state-owned enterprises, which is new and does not appear in TRIPS. [21]

It is clearly arguable that New Zealand law already complies with the TPPA civil law requirement, through the existing private law action for breach of confidence. New Zealand law complies with the TRIPS Agreement requirements and appears to be in compliance with the TPPA. New Zealand law protecting confidential information has traditionally been through the civil law protection provided through the action for breach of confidence, which is derived from English law. The common law action of breach of confidence is an action that generally has four elements: confidential information, an obligation not to disclose, unauthorised use or disclosure, and possible defences or justifications. [22] The action extends to cover not only situations in which information is confided, but also to cases of accidental or surreptitious acquisition of information, with knowledge that the information is confidential. [23] It also covers third-party receipt with knowledge. [24] Defences include a defence protecting disclosure in the public interest. [25] Importantly, a footnote to the TPPA article make clear that the article is without prejudice to a party's measures to protect good faith lawful disclosures providing evidence of violation of the party's laws. [26] This preserves aspects of the public interest defence and specific whistle-blower legislation, [27] although the public interest defence is wider, [28] and it is to be hoped that courts will not interpret the Agreement as narrowing the defence to these matters.

The civil law treats trade secrets as one category of confidential information. Trade secret issues commonly arise in the context of employment law, and particular approaches have been developed to protect trade secrets in an employment context. [29] The breach of confidence action is available for trade secrets, although there is no generally accepted definition of "trade secret" in this context. The breach of confidence action does not generally require that the courts identify whether the information meets some definition of trade secret, so long as the information has the necessary quality of confidence. [30] However, courts do from time to time use the term "trade secrets" to refer to commercial information. The concept of trade secrets as a category of information generally arises in case law in the context of employment. The issue of trade secrecy arises more specifically in cases involving restraints on ex-employees, where courts generally protect confidential information that is in the nature of a trade secret. [31] The law in this regard is not inconsistent with the civil law requirement in the TPPA.

The criminal law

There is a much more controversial criminal law requirement in the TPPA, which was not present in the TRIPS Agreement. Article 18(78)(2) of the TPPA requires parties to the agreement to provide for criminal procedures and penalties in relation to trade secrets. Again, in this context, the definition of "trade secrets" encompasses, at a minimum, undisclosed information as provided for in art.39(2) of the TRIPS Agreement. The TPPA provision states:
"Subject to Paragraph 3, each Party shall provide for criminal procedures and penalties for one or more of the following:
(a)
the unauthorized and wilful access to a trade secret held in a computer system;

(b)
the unauthorized and wilful misappropriation of a trade secret, including by means of a computer system; or

(c)
the fraudulent disclosure, or alternatively, the unauthorized and wilful disclosure, of a trade secret, including by means of a computer system."

Parties may deem "misappropriation" to be synonymous with "unlawful acquisition". [32]

Under TPPA art.18(78)(3), parties may limit the availability of criminal procedures, or limit the level of penalties available, to one or more of five cases. These are specified as follows:
(a)
"the acts are for purposes of commercial advantage or financial gain;

(b)
the acts are related to a product or service in national or international commerce; ***241**

(c)
the acts are intended to injure the owner of such trade secret;

(d)
the acts are directed by or for the benefit of or in association with a foreign economic entity; or

(e)
the acts are detrimental to a Party's economic interests, international relations, or national defense or national security."

A leaked earlier draft of the TPPA suggests that the criminal provision was a controversial inclusion, and also shows that it changed substantially in the course of negotiations. New Zealand appears to have supported at least some versions of the provision. [33] The provision requires all parties to provide criminal law protection in addition to civil law protection for trade secrets as defined in the TRIPS Agreement. Parties may choose to limit the action as provided, for example by requiring an intent to injure the owner, or to situations where there is an association with a foreign entity. Limitation may also be to cases of detriment to the economic interests, international relations, or national defence or national security of the state party.

Unlike Australia, New Zealand law does already provide for criminal law protection of trade secrets. The Crimes Act 1961 includes a provision prohibiting the taking of trade secrets, [34] and there are additional relevant provisions applying to unauthorised accessing of computer systems. [35]

Section 230 of the Crimes Act 1961

Section 230 of the Crimes Act 1961 [36] as amended in 2003 provides for an offence of taking, obtaining or copying trade secrets. The penalty on conviction is imprisonment for up to five years. Section 230 provides for a criminal offence:
"where a defendant takes, obtains or copies any document or any model or other depiction of any thing or process containing or embodying any trade secret, and

where a defendant takes or obtains *any copy* of any document or any model or other depiction of any thing or process containing or embodying any trade secret."

In both cases it is a requirement that:
the defendant has intent to obtain any pecuniary advantage or to cause loss to any other person;

the defendant has done the act of taking, obtaining or copying dishonestly and without claim of right;

the defendant must know that the document model or other depiction, or copy thereof, contains or embodies a trade secret.

In s.230 "trade secret" means any information that [37]
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 and the TPPA requirement differ in approach. Section 230 focuses on the taking, obtaining or copying of any document, model or other depiction of any thing or process containing or embodying any trade secret, or taking or obtaining *any copy* of a document, model or other depiction of any thing or process containing or embodying any trade secret. The section is not about protecting information that is a trade secret as such. It is only about protecting trade secrets where the secret is embodied in the document, model or other depiction of a thing or process. There is no definition of "taking", but it does not appear to extend to taking information without taking, obtaining or copying any document [38] or any model or other depiction. The section does not explicitly refer to disclosure of the trade secret, and disclosure is not in itself prohibited by the section. An act of disclosure is only likely to be caught under the section if there has also been an act of taking, obtaining or copying of the document, model or depiction. In this context, "obtain" has an extended meaning that includes "retain". [39] However, it is unlikely that it applies to retaining information if the document or any model or other depiction in which the trade secret is embodied is not also retained. Because of these important differences in approach, s.230 does not meet the TPPA requirement.

Section 249 of the Crimes Act 1961

The trade secret-specific provision in s.230 is complemented by other Crimes Act provisions designed to criminalise computer misuse. These provisions are generally targeted at computer hacking, but have been used more widely, including in cases akin to trade secret cases, some involving employees. Section 249 of the ***242** Crimes Act is a prohibition on accessing a computer system for a dishonest purpose. [40] Section 249 provides that:

(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; or

(b)

causes loss to any other person.

(2)

Every one is liable to imprisonment for a term not exceeding 5 years who, directly or indirectly, accesses any computer system with intent, dishonestly or by deception, and without claim of right,

(a)

to obtain any property, privilege, service, pecuniary advantage, benefit, or valuable consideration; or

(b)

to cause loss to any other person.

(3)

In this section, 'deception' has the same meaning as in section 240(2)."

The section provides for up to seven 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. Under s.249, it is an offence to access the computer system for a dishonest purpose to obtain "any property, privilege, service, pecuniary advantage, benefit, or valuable consideration; or causing loss to any other person". There is no need to establish that any information taken met 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). This is directed at conduct that involves an attempt. [41] Attempts to commit the offences in the section may also give rise to charges. [42]

Section 249 has been applied where information that might be regarded as a trade secret has been acquired from a computer system. It therefore, controversially, provides for parallel criminal law protection of trade secrets in those cases, and will catch employees taking information, as in the case of Watchorn v R., [43] in which an employee downloaded, but did not use, data from his employer's computer system. There had been some uncertainty around how the requirement of "obtaining any property, privilege, service, pecuniary advantage, benefit, or valuable consideration; or causing loss to any other person" applied in a context where information, such as a trade secret, has been taken. New Zealand courts had differed on whether information could be included in the definition of "property" as defined in the Crimes Act, so that the obtaining of information would constitute the obtaining of "property". [44] An alternative approach was the view that the taking of information could still be covered where the purpose was to obtain a "benefit". [45] The taking

of information could therefore be covered by the section if the information obtained was a "benefit". [46] The issue of whether in these cases information was "property" or a "benefit" under the section was resolved by a recent decision of the Supreme Court. [47] The Supreme Court held that digital files could be distinguished from pure information, and that digital files could be property for the purposes of s.249(1)(a). The Supreme Court was clear that it was not reconsidering the orthodox view that "pure information" was not property. [48] Digital files were distinguished from pure information, and the court considered that digital files could be identified, had a value and were capable of being transferred to others. [49] The Supreme Court therefore preferred the view that the taking of information from a computer in the form of digital files constituted the taking of property and not the acquiring of a benefit. [50] It is now clear that cases where trade secrets have been acquired from a computer system can be prosecuted under s.249, whether or not there is a financial advantage to the acquirer.

Section 249 meets some of the TPPA criminal law requirements but does not fully comply. Under the TPPA, each party is required to provide for criminal procedures or penalties in one or more of the specified situations. The first of these is "the unauthorised and wilful access to a trade secret held in a computer system". [51] Section 249(1) applies to directly or indirectly accessing any ***243** computer system. The section is not a match for the TPPA requirement. Section 249(1) is about accessing a computer system: there is no reference to accessing a trade secret in that computer system.

Section 249(1) requires not only the act of accessing the computer system but also 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. Section 249(1) may therefore prohibit at least some instances of the unauthorised, wilful access to a trade secret held in a computer system. However, s.249(1) will not apply to every instance where a trade secret is accessed wilfully and without authorisation. It will only apply where a computer system is accessed with intent, dishonestly or by deception, and property in the form of a data file or a benefit is obtained. The intent element is broadly similar to the requirement that it be wilful. The "dishonestly or by deception" element is not equivalent to "without authorisation". "Dishonestly", in relation to an act or omission, means done or omitted without a belief that there was express or implied consent to, or authority for, the act or omission from a person entitled to give such consent or authority. [52] It is therefore focused on the belief of the defendant rather than on whether there was authorisation. "Deception"' is also focused on the stage of mind of the defendant, it requires intent to deceive. [53] This is also a higher threshold than authorisation.

In summary, the requirements in s.249 have similarities to the TPPA provision relating to "unauthorized and wilful access to a trade secret held in a computer system", [54] but they are not equivalent. The thresholds for contravention on s.249 are higher than those in the TPPA. [55] The section does not meet the obligations in the TPPA, unless the limits on liability are within those permitted under art.18(78)(3).

Article 18(78)(3) of the TPPA sets out permitted limitations on the availability of criminal procedures or penalties. The only relevant permitted limitations are:
(a)
"the acts are for purposes of commercial advantage or financial gain;

and

(c)
the acts are intended to injure the owner of such trade secret."

Both (a) and (c) involve purpose or intent, and so the s.249(2) provision in relation to having the intent to do one of the prohibited acts is relevant here. The limitation in s.249, however, goes beyond the permitted limitation to the purposes

of commercial advantage or financial gain in subpara.(a). It provides for a limitation involving obtaining any property, privilege, service, pecuniary advantage, benefit or valuable consideration. This language clearly includes commercial advantage or financial gain, but is arguably wider, and may, for example, include a privilege or service that does not constitute commercial advantage or financial gain. This will be a matter for interpretation, and will depend on the approach taken in light of TPPA obligations. As already noted, the New Zealand Court of Appeal has said that benefit is not limited to financial advantage. [56] The Supreme Court referred to "benefit" as an "advantage", "good" or "profit". [57]

The limitation in s.249(2)(b) is also not within the permitted limitation in (c), as intent to injure the owner of such trade secret. There is an obvious issue here in that the use of the word "owner" is inconsistent with New Zealand law, in which information is clearly not property for these purposes. Arguably the use of "owner" can be regarded as metaphorical. [58] More serious is the problem about the scope of the limitation in s.249, which is wider than intent to injure the owner. The intent in s.249(2)(b) is accessing a computer system with intent, dishonestly or by deception, and without claim of right, to cause loss to any other person. Intent to cause loss is to any other person, not necessarily the owner. Additional elements are dishonesty or deception, and art.18(78)(3) does not extend to permitting limitations to conduct involving dishonesty or deception.

Section 252 of the Crimes Act 1961

Section 252 of the Crimes Act 1961 provides that:
(1)
"Every one is liable to imprisonment for a term not exceeding 2 years who intentionally accesses, directly or indirectly, any computer system without authorisation, knowing that he or she is not authorised to access that computer system, or being reckless as to whether or not he or she is authorised to access that computer system.

(2)
To avoid doubt, subsection (1) does not apply if a person who is authorised to access a computer system accesses that computer system for a purpose other than the one for which that person was given access. ***244** "

The requirements of the TPPA are also not met by s.252. It may apply in some cases in which a trade secret has been accessed wilfully and without authorisation, but it will not apply in all such cases. It proscribes intentionally accessing, directly or indirectly, any computer system without authorisation, where the person accessing the system knows that he or she is not authorised to access that computer system, or is reckless as to whether or not he or she is authorised to access that computer system. [59] The section makes no reference to accessing trade secrets. It does not apply if the person accessing the computer system is authorised to access a computer system and accesses that computer system for a purpose other than the one for which that person was given access. [60] This means that it does not apply to people such as employees who have authority to access the system but access it for another purpose, although this is a common fact pattern in civil trade secret cases.

Reforming the Crimes Act 1961

The requirements set out in the TPPA in relation to trade secrets are not met by the existing Crimes Act 1961 provisions. New Zealand will be required to amend its criminal law in order to comply. This presents an opportunity to review the existing criminal provision in s.230 of the Crimes Act 1961, and also to review the appropriateness and functionality of the application of the computer misuse provisions to trade secret-type cases.

Any criminal law protecting trade secrets is a supplement to the longstanding civil law regime. The civil law is a well-developed and nuanced regime that protects trade secrets but also has the capacity to protect the interests of employees,

the diffusion of information and the public interest on a case-by-case basis. The criminal law is less flexible and less well suited to accommodating competing values. There is also a risk that employees will face uncertain criminal liability for the acquisition of confidential information, even when such information has not been used or disclosed and there is no quantifiable loss to the employer. Jail terms become a possibility in such cases. [61] There is also a potential chilling effect on public disclosure of information that in the civil action would be covered by the public interest defence.

The problems inherent in criminalising trade secret protection mean that there are strong arguments for avoiding a maximalist approach to criminal protection of trade secrets. An approach targeted to the harm or harms identified is to be preferred. The rhetoric justifying increased trade secret protection is focused on cybersecurity and protecting trade secrets from outsiders, especially foreign hackers. [62] There is much less concern expressed about the threats from insiders such as confidants and employees. This suggests that the objective of the criminal provisions is primarily deterring and punishing economic espionage, especially foreign-based economic espionage. [63]

The TPPA offers a number of alternative approaches to the criminal protection of trade secrets, although some form of criminal protection is required. Parties to the Agreement may take a minimalist or maximalist approach. The flexibility is in two areas. First, parties can choose to provide criminal procedures and penalties for one or more of unauthorised wilful access, unauthorised wilful misappropriation, or fraudulent or unauthorised and wilful disclosure of a trade secret. A conservative approach would be to criminalise only fraudulent disclosure, leaving acts of access, misappropriation and or unauthorised and wilful disclosure without deception to be dealt with by the civil law. The second area of flexibility is on limitations on the availability of such procedures or penalties. Parties have the option to limit to one or more of five cases [64] and parties may impose some or all five limitations. The available limitations are specified as:
(a)
"the acts are for purposes of commercial advantage or financial gain;

(b)
the acts are related to a product or service in national or international commerce;

(c)
the acts are intended to injure the owner of such trade secret;

(d)
the acts are directed by or for the benefit of or in association with a foreign economic entity; or

(e)
the acts are detrimental to a Party's economic interests, international relations, or national defense or national security."

There are strong arguments for imposing four of these limitations within a redesigned New Zealand provision. Section 230 as it stands already requires intent elements, requiring intent to obtain any pecuniary advantage or to cause loss to any other person, and acting dishonestly and without claim of right. These limitations should be preserved, relying on the commercial advantage and intent to injure cases in (a) and (c). [65] Additionally, given that the concern is economic espionage, it is desirable that the new section be targeted at this harm, with a limitation to acts directed by or for the benefit of or in association with a foreign economic entity. This would exclude routine ***245** employee cases, except in the case where an employee took secrets for a foreign economic entity. Additionally, limiting liability to acts detrimental to a New Zealand's economic interests, international relations, or national defence or national security would assist in narrowing the focus to economic espionage contrary to the national interest.

A re-drafted trade secrets provision would therefore have the following elements:
It would prohibit the fraudulent disclosure of a trade secret, including by means of a computer system.

 © 2016 Thomson Reuters.

Criminal procedures and penalties would be limited to cases where:
the acts are for purposes of commercial advantage or financial gain and are intended to injure the owner of such trade secret;

the acts are directed by or for the benefit of or in association with a foreign economic entity; and are detrimental to New Zealand's economic interests, international relations, or national defence or national security.

This approach would narrow the existing provision in important ways, particularly to avoid use against employees that would be dealt with as a civil matter. It would be desirable to also redesign the computer misuse offences, especially s.249, which is not required under the TPPA, and as currently drafted has the potential to be used in trade secret cases, but does not offer the necessary protections for employees and freedom of expression values.

Conclusion

The TPPA obligations, if or when they come into force, will require a change in New Zealand criminal law relating to confidential commercial information and trade secrets. The obligations allow considerable flexibility in the design of the criminal provisions, and this presents an opportunity to review the existing provisions and to design new provisions based on coherent policy and closely targeted at the harms identified.

Dr Anna Kingsbury

University of Waikato, Hamilton

Footnotes

1 Associate Professor of Law, University of Waikato, Hamilton, New Zealand; Email: annak@waikato.ac.nz.

1 This is a particular concern in the US: see discussion in Zoe Argento, "Killing the Golden Goose: The Dangers of Strengthening Domestic Trade Secret Rights in Response to Cyber-Misappropriation" (2013–14) 16 Yale Journal of Law and Technology 172. Such concerns have also been raised in New Zealand: see for example the debates at the time of the 2013 amendments to the Government Communications Security Bureau Act 2003, which included changes to give greater prominence to the information assurance and cybersecurity functions of the GCSB to assist public sector entities and the private sector with information security. See Government Communications Security Bureau and Related Legislation Amendment Bill 2013 Explanatory Note, p.3, and Government Communications Security Bureau Act 2003 (as amended 2013) ss.7–8A

2 TRIPS Agreement art.39 requires that "Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices so long as such information:
(a)
is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;

(b)
has commercial value because it is secret; and

(c)
has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret."

3 The US Uniform Trade Secrets Act s.1(4) defines a "trade secret" as:
"Information, including a formula, pattern, compilation, program, device, method, technique, or process, that:
(i)
derives independent economic value, actual or potential, from not being generally known to or readily ascertainable through appropriate means by other persons who might obtain economic value from its disclosure or use; and

(ii)
is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."

4 Economic Espionage Act 1996 (18 USC §§1831–1839).

5 *H. Nasheri, Economic Espionage and Industrial Spying (Cambridge: Cambridge University Press, 2005), p.129*. The Act was amended in 2012 by the Theft of Trade Secrets Clarification Act, to extend coverage to products or services used in or intended for use in commerce. See §1832(a).

6 See proposed Defend Trade Secrets Act 2015 (H.R. 3326). The proposal has met with criticism. See for example David S. Levine and Sharon K. Sandeen, "Here Come the Trade Secret Trolls" (2015) 71 Washington & Lee Law Review Online 230; Christopher B. Seaman "The Case Against Federalizing Trade Secrecy" (2015) 101 Virginia Law Review 317; Argento, "Killing the Golden Goose" (2013–14) 16 Yale Journal of Law and Technology 172.

7 See Commission, Proposal for a Directive of the European Parliament and of the Council on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against their Unlawful Acquisition, Use and Disclosure (November 2013), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013PC0813 [Accessed 25 January 2016].

8 The European Parliament Committee on Industry, Research and Energy described the Directive as a benchmark in the context of negotiation of the Transatlantic Trade and Investment Partnership (TTIP). See Opinion on the Proposal for a Directive of the European Parliament and of the Council on the Protection of Undisclosed Know-how and Business Information (Trade Secrets) Against their Unlawful Acquisition, Use and Disclosure (29 April 2015), 3/52.

9 See discussion in Mark A. Lemley, "The Surprising Virtues of Treating Trade Secrets as IP Rights" (2008) 61 Stanford Law Review 311; Jonathan R.K. Stroud "The Tragedy of the Commons: A Hybrid Approach to Trade Secret Legal Theory" (2013) 12 Chicago-Kent Journal of Intellectual Property 232.

10 See for example discussion in Mars UK Ltd v Teknowledge Ltd [2000] F.S.R. 138 Ch D at [29]–[38], per Jacob J. Reverse-engineering is also permitted under the US Uniform Trade Secrets Act, but some aspects of it may be prohibited under the Economic Espionage Act. See discussion in Argento, "Killing the Golden Goose" (2013–14) 16 Yale Journal of Law and Technology 172, 186–187, 225–226.

11 The European Parliament Committee on Industry, Research and Energy produced an Opinion on the Proposal for a Directive of the European Parliament and of the Council on the Protection of Undisclosed Know-how and Business Information (Trade Secrets) Against their Unlawful Acquisition, Use and Disclosure (29 April 2015), 4/52, which refers to several studies demonstrating that regions/states enforcing strong non-compete agreements between employers and employees are subject to "brain drain" of the most highly skilled workers. See also discussion in Argento, "Killing the Golden Goose" (2013–14) 16 Yale Journal of Law and Technology 172, 183–185.

12 See Nedax Systems Ltd v Waterford Security Ltd [1994] 1 E.R.N.Z. 491 at 495, in which Goddard J said that "the right that employees have to leave their employment and to enter the employment of another employer or not, as they see fit, is so firmly established in our legal system that it is no exaggeration to call it a basic human right". See also Peninsula Real Estate v Harris [1992] 2 N.Z.L.R. 218, where Tipping J said that "In the absence of a restraint of trade clause a former employer cannot prevent a former employee simply from competing". This statement was adopted by Winkelmann J in SGS NZ Ltd v Nortel (1998) Ltd (High Court, Whangarei, CIV-2006-488-384, 20 December 2007) at [36].

13 See documents at http://ec.europa.eu/growth/industry/intellectual-property/trade-secrets/index_en.htm [Accessed 25 January 2016].

14 The proposed European Directive harmonises the civil law only. See Commission, Proposal for a Directive of the European Parliament and of the Council on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against their Unlawful Acquisition, Use and Disclosure

(November 2013), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013PC0813 [Accessed 25 January 2016]. The TPPA, however, includes criminal provisions.

15 The text of the TPPA is available on the New Zealand Ministry of Foreign Affairs and Trade website at http://www.mfat.govt.nz/Treaties-and-International-Law/01-Treaties-for-which-NZ-is-Depositary/0-Trans-Pacific-Partnership-Text.php. See also the description of the TPPA at http://www.tpp.mfat.govt.nz/ [Both accessed 25 January 2016].

16 See Trans-Pacific Partnership Ministers' Statement, http://www.tpp.mfat.govt.nz/assets/docs/TPP%20Ministers%20statement.pdf [Accessed 25 January 2016].

17 The text of the TPPA discussed in this article is from the intellectual property chapter released by New Zealand Ministry of Foreign Affairs and Trade, on their website at http://www.mfat.govt.nz/Treaties-and-International-Law/01-Treaties-for-which-NZ-is-Depositary/0-Trans-Pacific-Partnership-Text.php. The chapter was released earlier by Wikileaks. See "*TPP Treaty: Intellectual Property Rights Chapter, Consolidated Text (October 5 2015), Wikileaks release (October 9 2015)*, https://wikileaks.org/tpp-ip3/WikiLeaks-TPP-IP-Chapter/WikiLeaks-TPP-IP-Chapter-051015.pdf [Both accessed 25 January 2016].

18 Agreement on Trade-Related Aspects of Intellectual Property Rights 1994.

19 TRIPS Agreement art.39(2), fn.10.

20 TRIPS Agreement art.39(2). This definition has similarities with the US Uniform Trade Secrets Act definition of "trade secret", which defines the term as:
"information, including a formula, pattern, compilation, program, device, method, technique, or process,

that derives independent economic value, actual or potential, from not being generally known to or readily ascertainable through appropriate means by other persons who might obtain economic value from its disclosure or use; and

is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."

See *Uniform Trade Secrets Act with 1985 Amendments, Drafted by The National Conference of Commissioners On Uniform State Laws*, http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf [Accessed 25 January 2016].

21 See for example leaked text of the intellectual property chapter dated 30 August 2013, https://wikileaks.org/tpp/#sdfootnote251sym [Accessed 25 January 2016].

22 Coco v AN Clark Engineers Ltd [1969] R.P.C. 41 Ch D; AB Consolidated v Europe Strength Food Co Pty Ltd [1978] 2 N.Z.L.R. 515. See generally *Gurry on Breach of Confidence, 2nd edn, edited by T. Aplin, L. Bently, P. Johnson and S. Malynicz (Oxford: Oxford University Press, 2012), para.3-11*.

23 Attorney General v Guardian Newspapers Ltd (No.2) [1990] 1 A.C. 109 HL at 281–282; Franklin v Giddens [1978] Qd R. 72; Hunt v A [2008] 1 N.Z.L.R. 368. See also discussion in *Gurry on Breach of Confidence (2012), pp.263–286*.

24 Hunt v A [2008] 1 N.Z.L.R. 368; *Gurry on Breach of Confidence (2012), pp.286–300*.

25 Attorney-General for the United Kingdom v Wellington Newspapers Ltd [1988] 1 N.Z.L.R. 129 CA.

26 TPPA art.18(78), fn.135.

27 For New Zealand, see the Protected Disclosures Act 2000 (NZ).

28 See for example the application of the defence in Attorney-General for the United Kingdom v Wellington Newspapers Ltd [1988] 1 N.Z.L.R. 129; and New Zealand Post Ltd v Prebble [2001] N.Z.A.R. 360.

29 Faccenda Chicken v Fowler [1987] Ch. 117 CA (Civ Div); SSC & B: Lintas NZ Ltd v Murphy [1986] 2 N.Z.L.R. 436; Nedax Systems Ltd v Waterford Security Ltd [1994] 1 E.R.N.Z. 491; SGS NZ Ltd v Nortel (1998) Ltd (High Court, Whangarei, CIV-2006-488-384, 20 December 2007), Winkelmann J.

30 However, courts do from time to time use the term "trade secrets" to refer to commercial information. See discussion in *Gurry on Breach of Confidence (2012), pp.176–186*.

31 See Faccenda Chicken v Fowler [1987] Ch. 117. See also discussion in *Gurry on Breach of Confidence (2012), pp.509–539*.

32 TPPA art.18(78), fn.137.

33 See leaked text of the intellectual property chapter, "*WikiLeaks Release of Secret Trans-Pacific Partnership Agreement (TPP) Advanced Intellectual Property Chapter for All 12 Nations with Negotiating Positions*" *(30 August 2013, consolidated bracketed negotiating text)*, https://wikileaks.org/tpp/#sdfootnote251sym [Accessed 25 January 2016].

34 Crimes Act 1961 (NZ) s.230.

35 Crimes Act 1961 (NZ) ss.249 and 252.

36 Crimes Act 1961 (NZ) as amended 2003.
37 Crimes Act 1961 (NZ) s.230(2).
38 "Document" is defined broadly. See Crimes Act 1961 (NZ) s.217.
39 Crimes Act 1961 (NZ) s.217.
40 Crimes Act 1961 (NZ) s.249.
41 *Adams on Criminal Law, edited by Bruce Robertson (Thomson Reuters New Zealand, looseleaf), para.CA249.02*.
42 *Adams on Criminal Law (looseleaf), para.CA249.02, and para.72*.
43 Watchorn v R. [2014] NZCA 493. In the US, the (differently worded) Computer Fraud and Abuse Act 18 USC §1030 has been interpreted in some courts as applying to employees taking advantage of access privileges granted by their employers, but other courts have interpreted it as applying only to unauthorised access. See discussion in Argento, "Killing the Golden Goose" (2013–14) 16 Yale Journal of Law and Technology 172, 233–234.
44 Dixon v R. [2014] NZCA 329, [2014] 3 N.Z.L.R. 504 at [23]–[39]; Watchorn v R. [2014] NZCA 493 at [22]. Note that information is not generally regarded as property for civil law purposes. See discussion in *Paul Stanley, The Law of Confidentiality: A Restatement (Oxford; Portland, OR: Hart Publishing, 2008), pp.149–155*, See also *Gurry on Breach of Confidence (2012), pp.121–137*. See also discussion in Hunt v A [2008] 1 N.Z.L.R. 368 at [89]–[94].
45 Dixon v R. [2014] NZCA 329, [2014] 3 N.Z.L.R. 504; Watchorn v R. [2014] NZCA 493.
46 Watchorn v R. [2014] NZCA 493 at [81]. The Court of Appeal has said that "benefit" is not limited to financial advantage and has its normal meaning of anything that is of advantage to the person concerned.
47 Dixon v R. [2015] NZSC 147 (20 October 2015).
48 Dixon v R. [2015] NZSC 147 (20 October 2015) at [24].
49 Dixon v R. [2015] NZSC 147 (20 October 2015) at [25].
50 Dixon v R. [2015] NZSC 147 (20 October 2015) at [51]. The Supreme Court, at [54], said that it did not agree with the Court of Appeal finding that the digital files taken in R. v Watchorn were not property.
51 Trans Pacific Partnership Agreement art.18(78)(2)(a).
52 Crimes Act 1961 (NZ) s.217.
53 Crimes Act 1961 (NZ) s.249(3) provides that deception has the same meaning as in s.240(2). Section 240 defines "deception" as:
(a)
"a false representation, whether oral, documentary, or by conduct, where the person making the representation intends to deceive any other person and—
(i)
knows that it is false in a material particular; or

(ii)
is reckless as to whether it is false in a material particular; or

(b)
an omission to disclose a material particular, with intent to deceive any person, in circumstances where there is a duty to disclose it; or

(c)
a fraudulent device, trick, or stratagem used with intent to deceive any person."

54 Trans Pacific Partnership Agreement art.18(78)(2)(a).
55 Crimes Act s.249 will also not meet the requirements set out in the two other options for criminal procedures and penalties set out in Trans Pacific Partnership Agreement art.18(78)(2)(b) and (c).
56 Watchorn v R. [2014] NZCA 493 at [81].
57 Dixon v R. [2015] NZSC 147 (20 October 2015) at [51], referring to the *Shorter Oxford Dictionary, 6th edn (Oxford: Oxford University Press, 2007), p.220*.
58 *Gurry on Breach of Confidence (2012), p.121*.
59 Crimes Act 1961 (NZ) s.252(1).
60 Crimes Act 1961 (NZ) s.252(2).
61 Watchorn v R. [2014] NZCA 493 is an example.

62 See for example the debates at the time of the 2013 amendments to the Government Communications Security Bureau Act 2003, which included changes to give greater prominence to the information assurance and cybersecurity functions of the GCSB to assist public sector entities and the private sector with information security. See Government Communications Security Bureau and Related Legislation Amendment Bill 2013, Explanatory Note, p.3, and Government Communications Security Bureau Act 2003 (as amended 2013) ss.7–8A. The Government Communications Security Bureau Act now includes a National Cyber Security Centre: see http://www.ncsc.govt.nz/ [Accessed 25 January 2016].

63 See also discussion in A. **Kingsbury**, "Trade Secret Crime in New Zealand Law: What Was the Problem and is Criminalisation the Solution?" (2015) 37 E.I.P.R., 147.

64 Trans Pacific Partnership Agreement art.18(78)(3).

65 Trans Pacific Partnership Agreement art.18(78)(3)(a) and (c).

© 2016 Sweet & Maxwell and its Contributors

E.I.P.R. 2016, 38(4), 237-245

End of Document © 2016 Thomson Reuters.