Law and Society Association of Australia and New Zealand Conference 2015

THEME: Transgressing boundaries: regulation, emerging technologies and governmentalities

Cybersecurity, Moral Panics and the Law of Confidential Information

Anna Kingsbury.
Te Piringa Faculty of Law,
University of Waikato,
Hamilton, New Zealand

I. Introduction

This paper is about the trend to criminalisation of the protection of confidential information, and its justifications. In New Zealand as elsewhere, fears of foreign hackers and of breaches of national cybersecurity have been used to create a form of moral panic, justifying the extension of electronic surveillance by national security services. These same fears have also been used to justify the extension of the criminal law to the protection of confidential information and trade secrets. In the United States and in New Zealand, criminal offences have been creating prohibiting the taking of trade secrets, along with criminal offences relating to computer misuse. However, United States cases have involved United States employees, and in New Zealand these provisions have not led to prosecutions of foreign hackers, and such prosecutions would raise practical difficulties in any event. Employees and ex-employees appear to be much more likely defendants.

This paper discusses selected recent cases of theft of information by employees in knowledge-based industries in the United States, focusing particularly on cases involving scientists. New Zealand has as yet had few cases, but the paper discusses a recent case raising similar issues in a New Zealand context. The paper argues 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, particularly in the science-based industries.

II. Cybersecurity and Moral Panic

Cybersecurity has become a major preoccupation of the political classes in recent years. Cyber security concerns initially focussed more on the threat of computer hackers, who were generally characterised as malicious individuals rather than as trade competitors. Increasingly, however, concern has focussed on foreign economic espionage, the taking of information by foreign governments and foreign competitors. This is particularly evident in the United States, where economic espionage by Chinese interests has become a major political concern. These concerns have also been echoed in New Zealand political discussion and legislative debate. At an international level, arguments are increasingly being made for strengthening and harmonising trade secret protection.[1]

[1] For example, efforts are being made to include trade secret protection in the Trans-Pacific Partnership negotiations. See United States Chamber of Commerce, *The Case for Enhanced Protection of Trade Secrets in the Trans-Pacific Partnership Agreement.*

In recent years economic and industrial espionage or theft of trade secrets by foreign or domestic competitors has become a significant political issue in the United States. The taking of trade secrets by insiders and competitors is a long-standing issue. More recently, there has been growing concern about alleged economic espionage by foreign governments and companies in using computer technology to take trade secrets from United States companies.[2] Such foreign espionage is claimed to impose very significant costs on the United States economy.[3] Particular concern is expressed about the alleged activities of Chinese entities and the Chinese government in obtaining trade secrets.[4] In 2013 the United States administration produced a strategy to mitigate trade secret theft by foreign companies and foreign governments, with a particular but not exclusive focus on China.[5]

A consequence of growing concerns about cyber security and economic espionage is a renewed law enforcement interest in the taking of trade secrets. The United States Federal Bureau of Investigation (FBI) is active in investigating trade secret theft by foreign nationals and has identified economic espionage as its number two priority after terrorism.[6] The number of investigations has increased dramatically in recent years.[7] In addition to its investigative role, the FBI also runs a campaign to raise awareness of trade secret theft, and it maintains contact with businesses and academic institutions. It encourages affected companies and institutions to report possible trade secret theft to the FBI, in preference to bringing civil actions or using alternative approaches to resolution.[8] The FBI reports that economic espionage and theft of trade secrets involves both insiders, commonly employees, and cyber-enabled theft, such as hacking. Employees may steal for personal gain or to benefit another organisation or country.[9]

In New Zealand, cyber security, including the security of corporate trade secrets, has been used as a justification for expanding the powers of state security agencies. In 2013 amendments were made to the New Zealand Government Communications Security Bureau Act 2003, and these amendments included changes to give greater prominence to the information assurance and cybersecurity functions of the Government Communications Security Bureau to assist public sector

---

https://www.uschamber.com/sites/default/files/legacy/international/files/Final%20TPP%20Trade%20Secrets%208_0.pdf.

[2] See for example *The IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property* (2013) <http://www.ipcommission.org/> See also United States Chamber of Commerce, *The Case for Enhanced Protection of Trade Secrets in the Trans-Pacific Partnership Agreement* <http://www.amcham.or.id/images/amcham_updates/TPP%20Trade%20Secrets%20Study%208-19-13.pdf>

[3] One claim is that annual losses are likely to be over US$300 billion. See *The IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property* (2013) <http://www.ipcommission.org/>. page 2.

[4] See discussion in *The IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property* (2013) <http://www.ipcommission.org/>.

[5] Administration Strategy on Mitigating the Theft of U.S. Trade Secrets (February 2013) <http://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf>

[6] See <http://www.fbi.gov/about-us/investigate/counterintelligence/economic-espionage>. The FBI has indicted senior Chinese officials alleging trade secret theft. See <http://www.fbi.gov/wanted/cyber>

[7] In May 2014 Randall C. Coleman, Assistant Director of the FBI Counterintelligence Division reported in a Statement Before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism, that from the end of 2009 to the end of 2013 the number of economic espionage and theft of trade secrets cases overseen by the Economic Espionage Unit increased by more than 60 percent. See <http://www.fbi.gov/news/testimony/combating-economic-espionage-and-trade-secret-theft>

[8] See Randall C. Coleman, Assistant Director of the FBI Counterintelligence Division, Statement Before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism, May 13 2014, <http://www.fbi.gov/news/testimony/combating-economic-espionage-and-trade-secret-theft>

[9] See Randall C. Coleman, Assistant Director of the FBI Counterintelligence Division, Statement Before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism, May 13 2014, <http://www.fbi.gov/news/testimony/combating-economic-espionage-and-trade-secret-theft>

entities and the private sector with information security.[10] The security of information held by both government and private sector agencies is part of the work of the Government Communications Security Bureau, of which the National Cyber Security Centre is a division.[11] The agency's cyber-security role has been used to justify extending the powers of the agency.[12]

The rapid increase in concern about foreign economic espionage might be characterised as a form of moral panic. The concept of moral panic is used to describe a phenomenon in which a person, group, condition or episode becomes defined as a threat to society and becomes the subject of intense media attention and can lead to legislative change and changes to law enforcement policies and approaches.[13] The concept has been used to describe social and media reaction to computer hackers.[14] It might also be applied to the dramatic increase in law enforcement and media attention given to the threat of foreigners stealing trade secrets. However, despite the rhetoric about foreign threats, legislative and enforcement efforts are inevitably constrained by issues of jurisdiction and practical issues of enforcement against foreign-based hackers. Employees located within the jurisdiction are more likely targets for enforcement efforts, and the experience of case law to date seems to support this.

III. Legal protection of Confidential Information

The common law countries have for many years used the civil law to provide legal protection for confidential information, including information that could be described as a trade secret. 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.[15] New Zealand is one of few

[10] See Government Communications Security Bureau and Related Legislation Amendment Bill 2013 Explanatory Note, 3, and Government Communications Security Bureau Act 2003, (as amended 2013),ss 7-8A

[11] http://www.ncsc.govt.nz/

[12] The amendments extended powers of intelligence services justified in the basis of protecting cybersecurity and intellectual property. See the Government Communications Security Bureau Act 2003, as amended 2013, s 8A Information Assurance and Cybersecurity. See also discussion in Explanatory Note to the Government Communications Security Bureau and Related Legislation Amendment Bill 2013 109-1.

[13] On the concept of moral panic and its history, see generally C Krinsky (ed) *Ashgate Research Companion to Moral Panics* (2013), particularly pp 1-54, D Garland "On the Concept of Moral Panic" (2008) 4(1) *Crime Media Culture* 9-30. In relation to white collar crimes, see M Levi, "Suite Revenge? The Shaping of Folk Devils and Moral Panics about Whit-Collar Crimes" (2009) 49 *British Journal of Criminology*, 48-67.

[14] See for example A Ross "Hacking Away at the Counterculture" (1990) 1:1 *Postmodern Culture* 1, http://muse.jhu.edu/journals/postmodern_culture/v001/1.1ross.html

[15] Comments made in the Parliament in the course of debate on the legislation suggest that the provision was seen as a protection against economic espionage, and perhaps particularly economic espionage by foreigners. See speech by David Parker in *Parliamentary Debates (Hansard)* (12 June 2003) 609 NZPD 6238-6323. No empirical evidence was provided to establish that that foreign economic espionage actually constitutes a major threat to New Zealand companies. See discussion in A Kingsbury, "Trade Secret Crime in New Zealand Law: What Was the Problem and is Criminalisation the Solution?" (2015) 37:3 *European Intellectual Property Review 147.*

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.[16]

The United States has had a criminal provision covering the taking of trade secrets since 1997 In the United States, trade secrets are protected by both the civil and criminal law.[17] The United States had no federal criminal law protecting trade secrets until the passage of the Economic Espionage Act in 1996,[18] in force from 1 January 1997.[19] The Economic Espionage Act provided for a crime of economic espionage, which generally constitutes the taking, copying or receiving of a trade secret, intending or knowing that doing so will benefit a foreign government, foreign instrumentality or foreign agent. Penalties are fines of up to US$5 million or 15 years imprisonment or both for individuals, and for organisations, fines of up to US$10 million or 3 times the value of the stolen trade secret to the organisation.[20] It also provided for a crime of trade secret theft without a requirement of benefit to foreign entities. For this offence the penalties are fines and imprisonment of up to 10 years, and fines for organisations of up to US$5 million.[21]

IV. Legal protection of Confidential Information: The Case Law

There have been a number of recent prosecutions under the Economic Espionage Act 1996 that involved theft of trade secrets by employees. Examples include an action against former employees of Eli Lilly & Co for allegedly taking trade secrets, being information related to the development of new drug treatments, and passing the information to Chinese pharmaceutical producer.[22] The two scientists were reportedly Chinese nationals who had studied for doctorates in the United States and become United States citizens. The charges were brought in 2013, and eventually the prosecution requested they be dismissed in December 2014, after the scientists had spent time in jail and on home detention.[23] Other cases included one in which a former research scientist allegedly stole an anti-cancer compound,[24] one in which a research scientist pled guilty to taking confidential data

---

[16] There is no equivalent in Australia, the United Kingdom or Canada. A number of European countries have some criminal protection for trade secrets, but there is presently no Europe-wide provision, See Baker & McKenzie, *Study on Trade Secrets and Confidential Business Information in the Internal Market Final Study Prepared for the European Commission* (April 2013) pp 7-8 http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/130711_final-study_en.pdf

[17] Civil law breach of confidence was codified by statute since the 1979 approval of the Uniform Trade Secrets Act, which has been widely adopted across the United States. See discussion in R Denicola "The Restatements, the Uniform Act and the Status of American Trade Secret Law", in R Dreyfuss and K Strandburg (eds) *The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research (*2011) 18-45.

[18] Economic Espionage Act 1996 (18 US Code §§ 1831-39)

[19] H Nasheri, *Economic Espionage and Industrial Spying* (2005) 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)

[20] Economic Espionage Act 1996 (18 US Code §§ 1831)

[21] Economic Espionage Act 1996 (18 US Code §§ 1832) There is also provision for other orders including criminal forfeiture, orders to preserve confidentiality and injunctions in civil proceedings. Economic Espionage Act 1996 (18 US Code §§ 1834-6)

[22] *United States v Cao* No. 13 CR 00150 (S.D. Ind.) Discussed in J Schwartz et al, "2013 Trade Secrets Litigation Round-Up" *BNA's Patent Trademark and Copyright Journal* 87 PTCJ 717, 01/31/2014. Reproduced at <http://www.gibsondunn.com/publications/pages/2013-Trade-Secrets-Litigation-Round-Up.aspx>

[23] Jeff Swiatek and Kristine Guerra, "Feds dismiss charges against former Eli Lilly scientists accused of stealing trade secrets" December 5 2014, <http://www.indystar.com/story/news/crime/2014/12/05/feds-dismiss-charges-former-eli-lilly-scientists-accused-stealing-trade-secrets/19959235/>

[24] *United States v Zhao* No. 13 Cr. 00058 (E.D. Wis.) Discussed in J Schwartz et al, "2013 Trade Secrets Litigation Round-Up" *BNA's Patent Trademark and Copyright Journal* 87 PTCJ 717, 01/31/2014. Reproduced at <http://www.gibsondunn.com/publications/pages/2013-Trade-Secrets-Litigation-Round-Up.aspx>

from her employer, a pharmaceutical company,[25] and others involving taking of chemical formulae and data for use by foreign competitors.[26] In one widely reported case, a consultant, his company, and a California engineer were found guilty of economic espionage and trade secret theft in relation to information about a DuPont manufacturing process which was to be sold to a state-owned company in China.[27] The case was the first jury conviction on charges under the Economic Espionage Act in the United States. In July 2014 the Consultant, Mr Liew, was sentenced to 15 years in prison.[28]

Research scientists and engineers commonly have access to trade secrets, in both the public and private sectors, and this includes university researchers. In another widely reported United States case three New York University researchers in the NYU-Langone Medical Centre were charged in relation to sharing of trade secrets with a Chinese medical imaging company and government funded research laboratory.[29] The researchers worked on magnetic resonance imaging technology and had obtained a United States National Institutes of Health Research (NIH) grant to fund the research. The three were charged with taking bribes from a Chinese company, United Imaging Healthcare, in return for disclosing "certain research and non-public information" from the research at New York University funded by the NIH grant. The researchers were all Chinese citizens. The alleged bribes accepted included funding by the Chinese company of travel, US tuition fees and payment of rent on an apartment in New York. All three scientists allegedly maintained affiliations with United Imaging Healthcare and the Shenzhen Institutes of Advanced Technology, and these affiliations were not disclosed to NYU. One researcher also had a relevant patent that he allegedly did not disclose.[30] The case is still progressing through the courts at time of writing and so the final outcome is unknown.[31] However, the facts as stated raise some questions for university researchers with affiliations to more than one institution. It is increasingly common for academics to hold positions in more than one institution, and/or to work in collaboration with researchers from other institutions. A large proportion of the cases involve Chinese scientists with affiliations and relationships with Chinese companies and organisations, many funded by the Chinese government in efforts to develop research programs in China. However many researchers have joint affiliations with institutions in other countries, many in countries wishing to advance economic development, and in these situations similar divided loyalties and conflicts of interest can easily arise.[32] A particular concern is that in some cases people have been accused of theft of trade secrets on the basis of inaccurate information. This seems to have been the case for Dr Xi Xiaixing, a United

[25] *United States v Li* No. 3: 12-CR-00034 (D.N.J). Discussed in J Schwartz et al, "2012 Trade Secrets Litigation Round-Up" *BNA's Patent Trademark and Copyright Journal* 85 PTCJ 392, 01/18/2013. Reproduced at <http://www.gibsondunn.com/publications/Documents/2012TradeSecretsLitigationRoundUp.pdf >
See also <http://www.justice.gov/usao/nj/Press/files/pdffiles/2012/Li,%20Yuan%20Information.pdf>

[26] See for example *United States v Mohapatra* No. 1:11-CR-00132 (D. Utah), Discussed in J Schwartz et al, "2012 Trade Secrets Litigation Round-Up" *BNA's Patent Trademark and Copyright Journal* 85 PTCJ 392, 01/18/2013. Reproduced at <http://www.gibsondunn.com/publications/Documents/2012TradeSecretsLitigationRoundUp.pdf>

[27] *United States v Liew et al* No 3:11-CR-00573, (N.D.Cal),. See 2014 WL 2586329. See Karen Gullo, "California Man Guilty of Stealing DuPont Trade Secrets´ (March 6 2014) <http://www.bloomberg.com/news/2014-03-05/california-man-guilty-of-stealing-dupont-trade-secrets.html>

[28] See FBI Press Release: "Walter Liew Sentenced to 15 Years in Prison for Economic Espionage", July 11, 2014, <http://www.fbi.gov/sanfrancisco/press-releases/2014/walter-liew-sentenced-to-15-years-in-prison-for-economic-espionage>

[29] Benjamin Weiser, "3 NYU Scientists Accepted Bribes from China, US Says" *New York Times*, May 20 2013, <http://www.nytimes.com/2013/05/21/nyregion/us-says-3-nyu-scientists-took-bribes-to-reveal-work-to-china.html>

[30] *United States v Yudong Zhu, Xing Yang and Ye Li* No 13 Cr 000761 (S.D.N.Y.). See Complaint at <http://www.justice.gov/usao/nys/pressreleases/May13/ZhuYudongetalArrestsPR/U.S.%20v.%20Zhu,%20Yudong%20et%20al.%20Complaint.pdf>

[31] See *United States v Yudong Zhu* 23 F. Supp. 3d 234; 2014 U.S. Dist. LEXIS 77208, *United States v Yudong Zhu*, No 13 Cr 000761 (S.D.N.Y.) Dec 19 2014, see 2014 U.S. Dist. LEXIS 177796.

[32] See discussion in Christina Larson and Hao Xin, "Divided Loyalties Land Chinese Scientists in Hot Water" S*cience*, Vol. 340 no. 6136 pp. 1029-1031 (May 31 2013), <https://www.sciencemag.org/content/340/6136/1029.short?related-urls=yes&legid=sci;340/6136/1029>

States citizen and chair of the physics department at Temple University. He was arrested by the United States Justice Department and accused of sharing information with China, only to have the charges dropped months later when it was revealed that the information he had shared was not actually the secret design alleged to have been shared. The prosecutors had reportedly misunderstood the evidence.[33] In another recent case, a Chinese born hydrologist working for the National Weather Service in Ohio was arrested and accused of trade secret theft, only to have the charges dropped without explanation five months later.[34]

These cases evidence the law enforcement focus currently placed on trade secret protection, especially where there is a connection with China or Chinese interests. They also suggest that employees within the jurisdiction are likely to be subject to enforcement action, no doubt in many cases with justification. However, some of the cases also suggest that there is a risk to the science community that enforcement may be either excessive, or based on an inexpert understanding of the nature of the information allegedly taken. Law enforcement agencies will need expert advice on the precise nature of technical information and its status if mistakes are to be avoided.

New Zealand has not yet seen similar cases of criminal prosecutions of scientists, engineers and academics, but the United States cases demonstrate that criminal prosecution is a real possibility. Similar issues did arise however in one recent case. 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.[35] 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 $65,567 and penalties of $12,000.[36] In a subsequent criminal case, he 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 and 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 however 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. On the facts, 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. However this was not the end of the matter as a criminal trial and conviction followed. It is difficult to see the need for intervention of the criminal law in what is at heart an employment relationship dispute.

V. Conclusion

The moral panic around foreign economic espionage is greatest in the United States, but is not confined to the United States. It has led in part to criminalisation of trade secret protection in both the United States and New Zealand, and other jurisdictions will receive pressure to follow. The

[33] M Apuzzo, "US Drops Charges That Professor Shared Technology with China" New York Times Sept 11 2015.
[34] N Perlrith, "Accused of Spying for China, Until She Wasn't" New York Times, 9 May 2015.
[35] *Watchorn v R* [2014] NZCA 493
[36] *TAG Oil (NZ) Ltd v Watchorn* [2014] NZERA Wellington 58 5393742

existence and application of criminal provisions protecting trade secrets carries particular risks for employees, particularly employees working in science and in knowledge industries. For scientists, the risks are perhaps greatest. Scientists have a tradition of collaboration, and the line between confidential information and information which can be shared is not always entirely clear. For employees changing employers, there is a particular risk that they may take information claimed to be confidential. There is also a risk that law enforcement will misunderstand the distinction between confidential and non-confidential material, and misunderstand the technical nature of the information, as has happened in some of the United States cases. Law enforcement agencies are prioritising the area, and security services are active in detection. Scientists might have reason to feel considerable disquiet, and there is a potential impact on information-sharing and consequent innovation.

Cybersecurity, Moral Panics and the Law of Confidential Information

Anna Kingsbury.
Te Piringa Faculty of Law,
University of Waikato.

Cybersecurity As Moral Panic

- Moral panic: a phenomenon in which a person, group, condition or episode becomes defined as a threat to society and becomes the subject of intense media attention and can lead to legislative change and changes to law enforcement policies and approaches.
- Cybersecurity concerns as moral panic – particularly fear of foreign economic espionage
- Growing media attention and law enforcement responses

Rhetoric:

- Nationalistic rhetoric – IP Commission Report on "Theft of American intellectual Property", "Our" secrets/security
- Foreigners stealing our (corporate) trade secrets, foreign economic espionage, "cyber attacks", "cyber warfare" (where hackers working on behalf of foreign govts), "cyber threats"

Cybersecurity As Moral Panic

- Legislative reactions – especially criminalising the taking of corporate information
- TPPA requires criminal prohibition on the taking of trade secrets
- Growing concern of the criminal justice system
- Used to justify extensions to the surveillance powers of state security agencies to protect corporate trade secrets – characterised as "our" secrets
- "If New Zealand has secrets worth stealing,
  then they're worth protecting." (Ian Fletcher, Director GCSB, NZ)
- FBI: economic espionage is number 2 priority after terrorism. 2015 launched national awareness campaign on trade secret theft/economic espionage, using video. Focus on China

Trade Secrets: Criminal Law

United States

- Economic Espionage Act 1996
- Crime of economic espionage: the taking, copying or receiving of a trade secret, intending or knowing that doing so will benefit a foreign government, foreign instrumentality or foreign agent. Penalties are fines of up to US$5 million or 15 years imprisonment or both
- Crime of trade secret theft without a requirement of benefit to foreign entities. Penalties are fines and imprisonment of up to 10 years

New Zealand

- 2003 amendments to the Crimes Act 1961: new offences of taking, obtaining or copying of trade secrets Penalty imprisonment of up to 5 years
- Targeted at foreign hackers, but enforcement issues. Result is defendants are generally employees

May 19, 2014 12:00 PM
Five Chinese Military Hackers Charged with Cyber Espionage Against U.S.

From left, Chinese military officers Gu Chunhui, Huang Zhenyu, Sun Kailiang, Wang Dong, and Wen Xinyu have been indicted on cyber espionage charges.

Five Chinese military hackers were indicted on charges of computer hacking, economic espionage and other offenses directed at six American victims in the U.S. nuclear power, metals, and solar products industries. This marks the first time criminal charges have been filed against known state actors for hacking.

The Case Law: Science Employees

- Growing numbers of US cases against scientists, engineers, university academics alleging taking of trade secrets.
- Cases of Chinese scientists with affiliations and relationships with Chinese companies and organisations, many funded by the Chinese government in efforts to develop research programs in China. Some had done doctoral work in the US.
- Many researchers have joint affiliations with institutions in other countries, and in these situations similar divided loyalties and conflicts of interest can easily arise.

The Case Law: Science Employees: Examples

- 2013 three New York University researchers charged in relation to sharing of trade secrets with a Chinese medical imaging company and government funded research laboratory
- 2015, two Chinese professors among six defendants charged with economic espionage and theft of trade secrets in connection with their roles in a long-running effort to obtain U.S. trade secrets for the benefit of universities and companies controlled by the People's Republic of China (PRC).
- 2015 Dr Xi Xiaixing, a United States citizen and chair of the physics department at Temple University was arrested by the United States Justice Department and accused of sharing information with China, charges dropped months later when it was revealed that the information he had shared was not actually the secret design alleged.
- 2015 Chinese born hydrologist working for the National Weather Service in Ohio was arrested and accused of trade secret theft, only to have the charges dropped without explanation five months later.

The Case Law: Science Employees: Examples

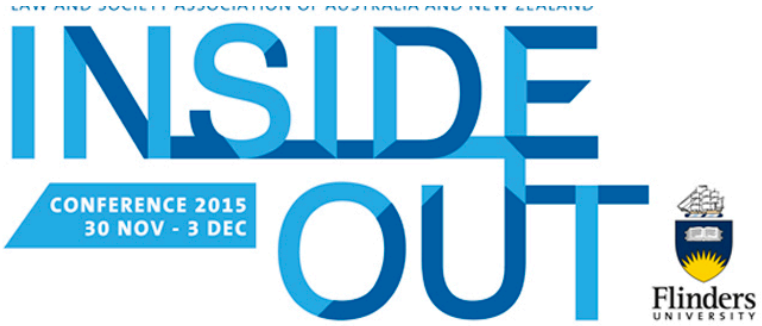
New Zealand :

- ***Watchorn v R* [2014] NZCA 493**
- James Watchorn, employee of TAG oil and gas exploration and mining company, had downloaded data from employer's computer system in anticipation of moving to another overseas employer, he had not misused the data. Employment Relations Authority awarded TAG special damages $65,567 and penalties of $12,000.
- Subsequent criminal case, he was convicted of accessing a computer system and thereby dishonestly and without claim of right obtaining property (or benefit), and was sentenced to two and a half years imprisonment (reduced on appeal so that served 5 weeks).
- NZ Supreme Court has since held that data is property, so that taking of data is taking of property (*Dixon v R* [2015] NZSC 147 20 October 2015)

Should we worry?

- Moral panic about cybersecurity has justified surveillance, and pattern of criminalising and enforcing criminal provisions applying to taking of employer information by employees
- Is it criminal? Is jail the right penalty? Is it an employment law/civil law issue?
- Problems of technical evidence, enforcement mistakes
- What information is protected? Definitions/clarity for employees and law enforcement.
- No public interest defence (whistleblowing)
- Chilling effect on science and scientific collaboration? Employee mobility.

SESSION TIMETABLE



Tuesday 1 December 2015

9.30–10.30am	**Registration and coffee**		
10.30–11.00am	**Welcome to country and opening**		
11.00–12.30pm	**Keynote: Is law inside or out? And why does it matter?** **Lynn Mather** **Room: 1.1**		
12.30–1.30pm	**Lunch**		
1.30–3.00pm	**Concurrent Session 1**		
Disability and Social Insurance **Room: 2.1** **Chair: Bridgette Toy-Cronin** ***Mariana Oppermann*** Madness inside and out the National Disability Insurance Scheme: structural impacts of the NDIS on social constructions of psychosocial disability ***Genevieve Grant & Emilie Friberg*** Diagnosing justice? Claimant encounters with officials in the Swedish social insurance system ***Warren Forster & Tom Barraclough*** Who gets to decide that your injury was caused by anything?	**Reason, Medicine and the Self** **Room: 2.2** **Chair: Katherine Curnow** ***Chris Dent*** Frankenstein's monster and the nineteenth century rise of the legal construct ***Colleen Davis*** Medical killings inside and outside the law of homicide ***Sue Jarrad*** Older persons and decision-making capacity: adaptations of law in the medical setting	**In and Out of Prison** **Room: 2.3** **Chair: Julian Murphy** ***Jeremy Ryder*** Artist, criminal, both? What impact does prisoners' artwork have on the outside? ***Carol Lawson*** Civil oversight: one size fits all? Insights from prison visitors in Japan and the ACT ***James Roffee*** Baseline sentencing: elite interviews and counter narratives	**Legal Geographies 1** **Room: 1.2** **Chair: Mary Spiers-Williams** ***Susan Bird, Malin Fransberg & Vesa Peipinen*** Urban wildscapes in Helsinki: exploring legal geographies in a DIY sauna ***Kim Economides*** Connecting law's internal and external spaces ***Shaun McVeigh*** Encounters of law and place – on the transport for London Bus Route number 68 from Norwood to Euston Station, taking in 'The BP exhibition: "Indigenous Australia: Enduring Civilization"' at the British Museum
3.00–3.30pm	**Afternoon Tea**		

3.30–5.00pm	Concurrent Session 2		
Justice at the End of Life **Room: 1.2** **Chair: Kathy Mack** ***Susannah Sage-Jacobson & Sue Jarrad*** Resolving disputes under the Advance Care Directives Act (SA) ***Katherine Curnow*** End of life decision-making: barriers to access to justice at a health provider level ***Pam Oliver*** 'All I want is to die peacefully': regulating for risk in assisted dying laws	**Rape and Sexual Violence** **Room: 2.1** **Chair: Jane Wangmann** ***Rachel Hirsch*** 'Don't mention the war': legal excising of footballer gang rape ***Robyn Holder & Kathleen Daly*** Money: exploring the meaning of financial assistance for survivors of sexual victimisation ***Heather Douglas*** Evidence and victim experience in sexual and domestic violence cases: the approach of the feminist judge	**Therapeutic Justice** **Room: 2.3** **Chair: Sharyn Roach Anleu** ***Danielle Misell*** The legal and therapeutic constructions of the appellant in *Habra v Police* ***Fiona Tait*** Testaments of transformation: the victim impact statement process in NSW as experienced by victims of crime ***Max Travers*** Business as usual? How magistrates make bail decisions in Tasmania	**Methodology and Ethics** **Room: 2.2** **Chair: Angela Melville** ***Genevieve Grant*** Getting bang for your data buck: empirical research using administrative and other existing data ***Olivera Simić*** 'Doing the research I do has left the scars': challenges of researching in transitional justice field
5.00–5.30pm	**Beverages**		
5.30–6.30pm	**Elliott Johnston Memorial Lecture: Why First Laws Must Be In** **Jacinta Ruru** **Pilgrim Uniting Church, 12 Flinders St (Opposite Flinders in Victoria Square)**		
6.30–7.00pm	**Canapes and Beverages**		

Wednesday 2 December 2015

8.30 – 9.30am	**Registration**			
9.30–11.00am	**Panel: How might we better engage Indigenous Knowledge in the academy and move towards putting the colonial imaginary of the savage to rest?** **Irene Watson, Marcelle Burns, Jen Nielsen** **Room: 1.1**			
11.00–11.30am	**Morning Tea**			
11.30am-1.00pm	**Concurrent Session 3**			
Children, Parents and Medical Interventions **Room: 1.2** **Chair: Jessie Hohmann** ***Travis Wisdom*** Children with intersex variations: legal regulation and human rights in Australia ***Fiona Kelly*** Transgender children and the Family Court ***Cornelia Koch*** Stop 'the chop'! The case for legal regulation of underage boys' circumcision ***Rachel Peterson*** The problematic assumption of the birth mother as legal parent in surrogacy agreements when using reproductive technologies in the UK	**Legal Education 1: Diversity** **Room: 2.1** **Chair: Ann Genovese** ***Dee Smythe*** Rhodes must fall! On teaching law (in context) in post-apartheid South Africa ***Anne Hewitt*** Empowering engagement: developing skills for embracing, celebrating and accommodating diversity in law school classrooms and beyond ***Angela Melville & Susana Arrese*** Teachers' perceptions of international student diversity: barriers, enrichment or self-actualisation? ***Jennifer Nielsen & Marcelle Burns*** Race and the law: a critical journey for law students	**Towards Transnational Approaches to Socio-legal Questions** **Room: 2.2** **Chair: Trish Luker** ***Mary Spiers Williams*** Mass incarceration of Aboriginal people in Australia: can law be emancipatory? ***Deirdre Howard-Wagner*** Indigenous practices inside and outside the court system in Newcastle, New South Wales ***Marium Jabyn*** Emancipatory politics, legal cultures and the international human rights regime ***Saptarshi Mandal*** Global governance, local feminisms: a case study of legislating domestic violence in India	**Family Violence** **Room: 1.1** **Chair: Heather Douglas** ***Robyn Holder, J. Putt & C. O'Leary*** The spaces between: advocating with and for Aboriginal women facing violence ***Rika Saraswati*** Legal space and its influence on access to justice for Indonesian women victims of domestic violence ***Katherine Kerr*** The dangerous impact of criminalising abortion: domestic violence and reproductive coercion	**Human Rights** **Room: 2.3** **Chair: Warren Forster** ***Laura Grenfell*** Systematic muting or systematic enhancing of human rights discourse? ***Damian Etone*** State engagement with the Universal Periodic Review (UPR): an added value to human rights monitoring mechanisms? ***Susan Peukert*** Reconceptualising the threshold test for coercive mental health treatment in light of Art 12 of the CRPD
1.00–2.00pm	**Lunch and LSAANZ AGM** (Room: 1.1)			

2.00–3.30pm	Concurrent Session 4		
Indigenous Legalities **Room: 2.1** **Chair: Dierdre Howard-Wagner** ***Stephen Young*** Native Title in an FPIC World: questioning the continued reliance on the right to negotiate ***Andie Palmer*** An indivisible and honourable Crown: a potential treaty partner for First Nations and Maori following the Mutua (Mau Mau) decision ***Jessie Hohmann*** Treaty as object, object as treaty: challenging the dichotomies of legal authority ***Sarah Ciftci*** Inside and outside of the circle: implications of culturally inclusive models for the broader decolonisation of Indigenous child welfare	**Constructing Legal Truths** **Room: 2.3** **Chair: Shaun McVeigh** ***Trish Luker*** Reading the archive: historians as expert witnesses ***Leah Findlay*** The new (140) characters in court reporting: media coverage of NSW criminal proceedings from colonisation to Web 2.0 ***Rob McQueen*** Transgressing boundaries on regulating rumours ***S Che Ekaratne*** More than moustaches: legal protections against unauthorised photo-manipulation in a technologically advanced society	**Legal Education 2: Preparing for Practice** **Room: 1.2** **Chair: Dee Smythe** ***Anne Hewitt*** Work integrated learning: educational panacea or poisoned chalice? ***Rachael Field*** Promoting law student wellbeing through the law curriculum: An ethical imperative for legal academics ***Francina Cantatore*** Joint initiatives: Using a pro bono teaching clinic to prepare law students for legal practice and promote community service	**Comparative and International Rights** **Room: 2.2** **Chair: Cristy Clark** ***Yun-Hsien Lin*** Gender equality agencies in an East Asian context ***Marium Jabyn*** Rights in 'principle' vs. rights in 'practice': the impact of CEDAW's Right to Public Life in the Maldives ***Catherine Renshaw*** Regionalism in the ordering of universal human rights
3.30–4.00pm	**Afternoon Tea**		
4.00–5.30pm	**Sub-Plenary Sessions**		
Major works in feminism and law: a 25 year anniversary celebration **Reg Graycar, Jenny Morgan, Ngaire Naffine, and Margaret Thornton** **Chair: Ann Genovese** Room: 1.2		**Earth jurisprudence: geography, science and property** **Nicole Graham, Lee Godden, John Page, Claire Williams** **Chair: Margaret Davies** Room: 2.1	
6.30–11.30pm	**Conference Dinner**		

Thursday 3 December 2015

8.30 – 9.30am	**Registration**		
9.30–11.00am	**Sub-Plenary Sessions**		
A dialogical encounter of ethical futures (The existential threat: how do you bring wisdom to the table?) **Christine Black and Olivia Barr** **Room: 1.2**		**Decriminalising abortion** **Barbara Baird, Mark Rankin, Clare Parker, Sally Sheldon** **Chair: Mary Heath** **Room: 2.1**	
11:00–11.15am	**Morning Tea**		
11.15–12.45pm	**Concurrent Session 5**		
Commerce and Tax **Room: 2.2** **Chair: Margaret Davies** ***Nikola Georgiev*** Principle of autonomy in Letter of Credit (LC): an overview from legal and shariah perspective ***Megan Vine*** Wine Equalisation Tax Rebate: rethinking the legal framework in a social, environmental and economic context ***Chilenye Nwapi*** The significance of mining codes in Africa for company–community relations and social licence to operate	**Theorising Law's Insides and Outsides** **Room: 2.3** **Chair: Jen Nielsen** ***Rhys Aston*** Anarchism, law and social change ***Timothy Peters*** Turning corporate law inside out: a political theology of the corporate body ***Saika Sabir*** Using intersectionality in the 'post-period': law, gender and identity politics in contemporary India technologically advanced society	**Women's Health Law** **Room: 2.1** **Chair: Sally Sheldon** ***Suzanne Belton*** Transforming the *Medical Services Act* in the Northern Territory: the frontiers of feminist law advocacy ***Suzanne Belton & Virginia Skinner*** Transforming the *Medical Services Act* in the Northern Territory: making laws that work for women and health practitioners ***Felicity Gerry*** Don't blame the parents: female genital mutilation and how campaigners have succeeded where law and policy feared to tread ***Anna O'Rourke*** Legal strategies of anti-abortion activists in Australia	**Courts, Activism and Access** **Room: 1.2** **Chair: Robyn Holder** ***Tanya Josev*** Is 'activism' a dirty word now? The campaign against activism in the courts ***Bridgette Toy-Cronin*** A limited welcome: methods and motives for communicating outsider status to litigants in person ***Lisa Webley*** When is a family lawyer, a lawyer? ***John Flood*** Form and substance in lawyer–client relationships
12.45–1.30pm	**Lunch**		

1.30–3.00pm	Concurrent Session 6		
Legal Geographies 2 **Room: 2.3** **Chair: Nicole Graham** ***Brendan Grigg*** Legal time warps and obesogenic environments: slow law/fast food ***Lauren Butterly*** Dipping your toes into legal geography: governing sea country spaces in Australia ***Julian Murphy*** Architecting access to justice: the courts as doors to the law	**Work-Life Balance in the Legal Profession and Judiciary** **Room: 2.1** **Chair: John Flood** ***Richard Collier & Margaret Thornton*** Balancing on a tightrope: law and life in the legal profession ***Kathy Mack & Sharyn Roach Anleu*** Managing work and family in the Australian judiciary: metaphors and strategies	**The Legal Limits of State Power** **Room: 2.2** **Chair: Chilenye Nwapi** ***Anna Kingsbury*** Cybersecurity, moral panics and the law of confidential information ***Andrew Kenyon*** A state of affairs of freedom implications of media and free speech in German law ***Sascha Mueller*** Codifying extraordinary powers: furthering democracy or executive creep?	**Miscarriages of Justice** **Room: 1.2** **Chair: Tim Peters** ***Kevin Borick*** A fair trial is a basic human right ***Bibi Sangha & Robert Moles*** Miscarriages of justice and the statutory right to a second or further appeal in South Australia.
3.00–3.15pm	**Afternoon Tea**		
3.15–4.00pm	**Closing Plenary: Law's Aliens** **Margaret Davies** **Room: 1.1**		
4.00–4.30pm	**Conference Wrap Up**		