SHIELDING CRITICAL INFRASTRUCTURE INFORMATION-SHARING SCHEMES FROM COMPETITION LAW

STEPHEN CORONES AND BILL LANE*

Because the majority of critical infrastructure is now owned or operated by the private sector, governments have implemented schemes to facilitate the exchange of information between private sector owners and operators, to ensure that it is protected from terrorist attack. The operation of these information-sharing schemes has the potential to contravene the competition law provisions contained in Division 1 and Division 2 of Part IV of the Trade Practices Act 1974 *(Cth) (TPA). In light of these matters, this article considers whether there is a need for a specific statutory defence in the TPA in order to ensure that such arrangements can operate effectively and encourage the frank exchange of this type of information. The article examines the existing voluntary self-regulatory scheme adopted in Australia in 2003 and compares it with similar schemes in the United States where there is a move away from voluntary self-regulation towards a mandatory regulatory model with a specific legislated defence to shield critical infrastructure information-exchange arrangements from antitrust laws.*

I INTRODUCTION

A Threats to Critical Infrastructure

Following the terrorist attacks in the United States of America on September 11, 2001, and subsequent terrorist attacks in Bali (2002), Madrid (2004), London (2005), Mumbai (2008), and Jakarta (2009), there has been an increasing recognition by governments world-wide of the heightened importance of ensuring that adequate protection exists for critical

* Stephen Corones, Professor of Law, Faculty of Law, Queensland University of Technology; Bill Lane, Clayton Utz Professor of Public Law, Queensland University of Technology.

This research was supported by a grant from the Australian Research Council – DP 0773706. We have benefited from discussions with Professor Ed Dawson, Dr Jason Reid and Dr Jason Smith of the Information Security Institute, Faculty of Information Technology, Queensland University of Technology.

infrastructure. 'Critical Infrastructure' (CI) is defined by the Australian Government as:

> those physical facilities, supply chains, information technologies and communications networks which, if destroyed, degraded or rendered unavailable for an extended period, would adversely impact on the social or economic well-being of the nation or affect Australia's ability to ensure national security.[1]

The enduring threat of terrorist attacks in Australia was acknowledged by the then Prime Minister as recently as August 2009, following the arrest of Somali extremists who were allegedly planning a terrorist attack on the Holsworthy army base in Sydney.[2] On 16 October 2009, the five extremists were convicted of terrorism offences. The judge found that that there was no evidence of any target having been selected; however, this did not mitigate the criminality of the terrorists in preparing for such an act. The terrorists had stockpiled 30 000 rounds of ammunition, bomb-making equipment and explosive chemicals with the intention of exacting revenge on Australia for its military presence in Iraq and Afghanistan.[3]

Digital infrastructure is especially vulnerable to attack. Cyber attacks are difficult to detect and even harder to defend against. The implications of a cyber attack via the internet could result in: the collapse of communications networks; the failure of electronic banking and major online shops including eBay and Amazon; the failure of transport networks, including air traffic control computers and railway systems; and the failure of the electricity grid, shutting down power supplies and causing widespread blackouts.[4] In the United States researchers have launched an experimental cyber attack which caused an electricity generator to self-destruct.[5]

---

[1] Attorney-General's Department, *Critical Infrastructure Protection* (2009) <http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_CriticalInfrastructureProtection>.

[2] Cameron Stewart and Milanda Rout, 'Somali extremists on a "fatwa order" from God': *The Australian* (Sydney) 5 August 2009, 4.

[3] James Madden and Angus Thompson, 'Sydney Terror quintet facing life in jail for plotting murder on a massive scale', *The Australian* (Sydney) 17 October 2009, 1; Sally Neighbour, 'Delusions of terror', *The Australian* (Sydney), 20 October 2009, 13.

[4] 'On the cyberwar's frontline', *The Guardian Weekly* (Haywards Heath, UK) 22 May 2009, 25.

[5] Jeanne Meserve, *Sources: Staged cyber attack reveals vulnerability in power grid* (26 September 2007) CNN International < http://edition.cnn.com/2007/US/09/26/power.at.risk/index.html> and Industrial Defender, *Optimized to Assure Safety and Uptime* (2010) <http://www.industrialdefender.com/compliance/index.php>.

The vulnerabilities of CI, and the growing capabilities and commitment of terrorists to inflict harm, are a continuing cause for concern on the part of government and private sector owners and operators of CI. Establishing an effective means of sharing of physical and cyber security information through the operation of CI information sharing schemes ('CIISS') has become an important component of effective CI and cyber-security risk management.

B Responses to the Threat

On 29 May 2009, President Obama presented the Cyberspace Policy Review[6] which reports on the changing direction of US cyber-security under the Obama administration. It states that cyber-security risks '... pose some of the most serious economic and national security challenges of the 21st century'.[7] The President has assumed responsibility for cyber-security. A national cyber-security coordinator is to be appointed to oversee the task and report directly to the President.

Australia is in the early stages of developing an information sharing network to combat terrorist attacks. The Trusted Information Sharing Network for Critical Infrastructure Protection ('TISN') was launched by the Commonwealth in 2003 to provide a secure forum for owners and operators of CI and government stakeholders to share information and discuss issues.

Participation in the TISN is voluntary. Information is disclosed at the discretion of each private participant, although they are required to sign a deed of confidentiality. It is unclear what sort of information is exchanged. Some guidance is provided by the cyber exercise program conducted by the Attorney-General's Department, Security and Critical Infrastructure Division from 10-14 March 2008 (Cyber Storm II).[8] The purpose of the program was to improve the ability of governments and CI owners and operators to manage and respond to incidents affecting national infrastructure.

The Cyber Storm II exercise involved four CI sectors – Water, Banking and Finance, Energy and Communications. According to the Final Report, the exercise 'enabled robust information sharing, and encouraged private-public sector relationships and coordination across industries and between

---

[6] White House, *Cyberspace Policy Review* (2009) <http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>.

[7] Ibid iii.

[8] See Attorney-General's Department, Security and Critical Infrastructure Division, *Cyber Storm II National Cyber Security Exercise Final Report* (August 2008) <http://www.tisn.gov.au/www/tisn/rwpattach.nsf/VAP/(99292794923AE8E7CBABC6FB71541EE1)~Cyber+Storm+II+final+report.pdf/$file/Cyber+Storm+II+final+report.pdf >.

competitors'.[9] Participants enacted 12 simulated scenarios, including widespread internet degradation. Cyber Storm II allowed the participants to 'run an internal e-security exercise in conjunction with many of their suppliers and/or customers'.[10]

C Conflict with Existing Legal Regimes

Any CIISS must take account of existing legal regimes. There are currently a number of legal and related issues that can impede effective information-sharing arrangements pursuant to a CIISS.[11]

Information-sharing of the very kind for which a CIISS is established (that concerning security matters) may directly interfere with competition between participants. Obviously, much security information will deal with issues of competitor vulnerability and reliability – that is, information about known risk exposures and post-incident response planning to ensure that services will continue to be provided even under adverse circumstances. Where operators of CI compete with each other, the reliability of their services is one way in which competitive rivalry manifests itself.

Exclusive possession of such security information gives a firm a competitive advantage over its rivals, in that its services will be more reliable than those of its rivals. If Bank A's EFTPOS processing network becomes unreliable, its clients are likely to change to other banks. If Bank B possesses information which makes its service more reliable, then by sharing this information with Bank A, Bank B could forgo this competitive advantage.

Given these disadvantages, governments need to ensure that adequate incentives exist for CI owners and operators to share information and that existing laws do not operate as an impediment to the sharing of such information.[12]

---

[9] Ibid 8.

[10] Ibid 7.

[11] See, for example, Bill Lane et al, 'Freedom of information implications of information sharing networks for critical infrastructure protection' (2008) 15(4) *Australian Journal of Administrative Law* 193.

[12] See Amitai Aviram and Avishalom Tor, *Information Sharing in Critical Infrastructure Industries: Understanding the Behavioural and Economic Impediments* (23 February 2004) Social Science Research Network <http://ssrn.com/abstract=427540>. See also John Han, 'Antitrust and Sharing Information about Product Quality' (2006) 73 *University of Chicago Law Review* 995 and Amitai Aviram and Avishalom Tor, 'Overcoming Impediments to Information Sharing' (2004) 55 *Alabama Law Review* 231.

D Security Information and the Trade Practices Act

This article seeks to examine the risk that sharing the kinds of information set out above or just 'security information' may breach Divisions 1 and 2 of Part IV of the *Trade Practices Act 1974* (Cth) (TPA).

In the first part of the article we examine the information-sharing schemes that have been adopted in the United States and Australia for protecting CI and cyber-security. Next, we consider the risks and uncertainty surrounding the application of Divisions 1 and 2 of Part IV of the TPA to the existing TISN and any possible expansion of TISN-related activities. The central theme of this article is that this uncertainty should be eliminated since it has the capacity to inhibit effective participation in a CIISS by private sector participants. In the final part of the article we consider three mechanisms by which immunity could be conferred on private sector participants in CIISS activities.

There is now broad agreement with the underlying policy against anti-competitive practices enshrined in Part IV of the TPA. However, it is also recognised that in some circumstances protecting competition must give way to other social policy objectives.

II PUBLIC/PRIVATE PERSPECTIVES, REGULATORY APPROACHES AND TYPES OF INFORMATION SHARED

CI protection and cyber-security involve two competing perspectives. On the one hand, governments bear responsibility for the maintenance of law and order and the protection of persons and property. Moreover, to the extent that the danger of terrorist attack emanates from or is linked to forces external to Australia, it is the responsibility of the Australian Federal government to protect its citizens from external threats to security. On the other hand, whilst governments and individuals alike rely heavily on CI for many essential services, up to 90 per cent of CI is actually privately owned.

The different perspectives of business and government mean that each sector is likely to have a different conception of risk. While the owners and operators of CI have a sufficient incentive to protect their assets from terrorist attack, government reliance on CI means that it is likely to be relatively more risk-averse and thus inclined to intervene to ensure that private owners and operators have adopted adequate standards and measures of protection. Even where the risk of a terrorist attack is perceived to be low, the consequences can be so severe that, from a public perspective, any level of risk is unacceptable.

Anderson and Fuloria make the argument for government regulatory intervention on the basis of 'the large externalities of correlated failure'.[13] While a single-incident attack on an oil refinery could be accommodated by the oil company and its insurers, a multiple-incident attack on several oil refineries would cause a major disruption requiring government intervention. They draw an analogy with financial regulation: the isolated failure of a single bank may be of little consequence; but the risk of correlated failure imposes large externalities.

A Models of CI Protection

There are a range of possible models for CI protection.[14] At one end of the spectrum, especially where CI assets are in government ownership, the government can directly mandate CI protection requirements by establishing its own cyber-security standards or at least delegating that responsibility to public regulatory agencies. At the other end of the spectrum, especially where CI is privately owned or controlled, regulation may be less direct or interventionist – involving, for example, various forms of voluntary self-regulation.

Beyond this, as the Cyberspace Policy Review[15] recognises, cyber-security is inevitably a shared responsibility, requiring a collaborative partnership to protect public and private interests. In other words, CI protection in most cases is likely to be a public-private partnership by government and the private sector owners of infrastructure, involving a system of information-sharing and co-ordinated response. In fact, this is the approach taken in Australia – as explained earlier, the TISN was established by the Federal government in 2003 to provide a secure forum in which owners and operators of CI and government stakeholders can share information and discuss issues.

B Information Sharing

Essentially, information-sharing arrangements for CI protection involve the exchange of information between CI owners or operators. This information is considered to be of mutual benefit in identifying and dealing effectively with

---

[13] Ross Anderson and Shailendra Fuloria, *Security economics and Critical National Infrastructure* <http://weis09.infosecon.net/files/124/paper124.pdf>.

[14] Dan Assaf, 'Models of critical information infrastructure protection' 1 (2008) *International Journal of Critical Infrastructure Protection* 6. See also Critical Infrastructure Protection Program, *The CIP Report: Volume 6 Number 12* (June 2008) <http://cip.gmu.edu/archive/cip_report_6.12.pdf> which contains short descriptions of CIIP regimes in Israel, Sweden, United Kingdom, the European Union.

[15] White House, above n 6.

risks of attack or interference. Clearly, the viability of such arrangements is dependent on the confidentiality of exchanges. This confidentiality is necessary for obvious security reasons but also to ensure that participants are not inhibited from full and frank exchanges.

This means, of course, that the ability to accurately identify or predict the exact nature and type of information likely to be shared in such an arrangement is very limited. Nevertheless, the general significance of private sector arrangements of this nature is obvious – in particular, their potential to operate in a realm unhindered by the possible reach of relevant TPA restrictions, especially those intended to regulate private sector business arrangements likely to result in anti-competitive practices.

On that basis, it is important at least to postulate the types of information likely to be shared in order to properly analyse the consequences produced by information-sharing arrangements of this type for the scope and operation of the TPA and the balancing of competing interests.

Accordingly and for the purposes of our analysis, we have postulated two broad categories of information likely to be shared if a CIISS is to be effective as a mechanism for identifying and dealing with security risks:

Category 1: Pre-incident information exchange to prevent or minimise the risk of terrorist attack

This category consists of:

- Information to assist in identifying vulnerabilities; threat intelligence; information about existing security technologies and possible future technologies and best practices and risk management strategies.

- Information to assist in preventing attacks, including interdependencies, inter-operability and compatibility of existing technologies and product characteristics which allow for coordination across industries and between competitors, supplier and/or customers.

- 'Incident information' concerning existing attacks or attempts to disrupt infrastructure systems, whether the incident is cyber or physical.

Category 2: Post-incident response planning information exchange

This category consists of:

- Information and action plans designed to ensure business continuity, including information about production capacity, inventory stock levels and alternative supply arrangements involving potential allocations of scarce commodities, including both supplies for repair, and customer products to cover disabled or destroyed CI.

The most serious risks of contravening Part IV of the TPA arise from the sharing of Category 2 information, especially information about production and inventory stock levels, future output plans, the rationing of available supplies, the sharing of spare parts to repair damaged CI following an attack and the allocation of products to existing customers.

Moreover, following an attack in a particular region, private sector operators may stop competing with each other and instead agree to collectively focus their attention on supplying the affected region, particular customers or particular recovery projects in the region. They may also collectively agree to ration scarce supplies.

The significance of this is that measures such as these are likely to satisfy the definition of a cartel provision in section 44ZZRD(3)(a)(iii) of the TPA. They are also likely to satisfy the definition of an exclusionary provision in section 4D of the TPA, even though the main purpose is to restore the region to normality as quickly as possible.

III INFORMATION-SHARING SCHEMES FOR CRITICAL INFRASTRUCTURE PROTECTION: US AND AUSTRALIA COMPARED

As indicated earlier, the approach adopted by the governments of Australia and the United States is to protect their CI by facilitating the sharing of relevant information between CI operators on the one hand, and government on the other. These information-sharing schemes typically involve a combination of face-to-face meetings and electronic information exchange. In this Part we consider the approach adopted in the United States and then compare it with the approach adopted in Australia.

A United States of America

The model adopted in the United States is one of industry sector, voluntary, self-regulation. The necessity for public-private collaboration and information-sharing to protect critical infrastructure was recognised as early as 1997 in the report of the President's Commission on Critical Infrastructure. Presidential directive PD-63 issued by President Clinton in 1998 called for the creation of Information Sharing and Analysis Centres (ISACs) to protect the nation's critical infrastructures by gathering, analysing, and disseminating information when appropriate.[16] It was thought that this would foster voluntary self-regulation.

In response to the Directive, the financial services industry formed the FS-ISAC (Financial Services Information Sharing and Analysis Centre) in 1999.[17] This was followed in 2001, by the IT-ISAC (Information Technology Information Sharing and Analysis Centre), formed by 19 prominent IT companies. Each group uses a central repository to store and distribute information about security vulnerabilities and attacks, and members are expected to report information concerning their security problems or the solutions they have devised to such problems.

Overall responsibility for initiating a critical infrastructure protection program in the United States, including information-sharing, has been assumed by the President, in conjunction with the Department of Homeland Security.[18] The resulting Protected Critical Infrastructure Information Program is intended to be an information-sharing network between the private sector and government with capability to investigate and analyse vulnerabilities and risk assessments and discuss and implement greater CI protection.[19]

As part of the program, the Critical Infrastructure Partnership Advisory Council oversees separate industry-sector and government-sector committees.[20] Representatives from all committees sit on the Advisory Council which aims to engage all participants and provide overall direction and guidance. There are 16 sector committees which have industry and

---

[16] Clinton Administration, *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63* (22 May 1998) Federation of American Scientists <http://www.fas.org/irp/offdocs/paper598.htm>.

[17] Information about FS-ISAC can be obtained from its website at: Financial Services Information Sharing and Analysis Centre, *Financial Services Information Sharing and Analysis Centre* <http://www.fsisac.com>.

[18] 6 USC §132 (2000).

[19] Homeland Security, *Protected Critical Infrastructure Information Program* (8 December 2009) <http://www.dhs.gov/xinfoshare/programs/editorial_0404.shtm>.

[20] Ibid.

government members. These cover chemical and commercial facilities, communications, dams, defence, electricity, emergency services, financial services, food and agriculture, healthcare and public health, information technology, nuclear facilities, oil and natural gas, postal and shipping services, transportation and water. There are also State, Local, Tribal and Territorial government committees.[21]

The United States is moving away from the voluntary self-regulation model towards a mandatory regulatory model.[22] The *Homeland Security Appropriations Act 2007* authorised the Department of Homeland Security to promulgate mandatory regulations, including cyber-security regulations, for securing high-risk chemicals.[23]

Similar mandatory cyber-security standards have been promulgated for the energy sector under the *Energy Policy Act 2005* (US). The North-American Electric Reliability Corporation (NERC) has developed cyber-security standards for the energy sector ISAC. These standards have received the approval of the Federal Energy Regulatory Commission (FERC) and are now mandatory.[24]

The fear of intervention by competition regulators may operate as a disincentive to effective participation in a CIISS. In its 2003 report, a committee of the US National Research Council asserted that '[m]any companies fear that sharing [CI protection]-related data with competitors could be viewed as a violation of the antitrust provisions of the Sherman Act'.[25]

Information-sharing agreements run the risk of being unlawful under section 1 of the *Sherman Act*, which prohibits all agreements in restraint of trade. Communications falling short of an agreement may constitute a 'facilitating

---

[21] Homeland Security, *Council Members, Critical Infrastructure Partnership Advisory Council* (3 June 2009) <http://www.dhs.gov/xprevprot/committees/editorial_0848.shtm>. Information about ISAC council is available from its website at: ISAC Council, *About the Council* <http://www.isaccouncil.org>.

[22] Dan Assaf, 'Models of critical information infrastructure protection' 1 (2008) *International Journal of Critical Infrastructure Protection* 6.

[23] *Homeland Security Appropriations Act 2007*, Pub L No 109-295, § 550, 120 Stat 1355, 1388.The chemical standards are available at: Industrial Defender, *NERC CIP Compliance Solutions* (2010) <http://www.industrialdefender.com/compliance/nerc_resources.php>.

[24] The NERC standards are available at: North American Electric Reliability Corporation, *Reliability Standards* (2010) <http://www.nerc.com/page.php?cid=2|20>.

[25] Stewart Personick and Cynthia Patterson (eds), *Critical Information Infrastructure Protection and the Law: An Overview of Key Issues* (The National Academies Press, 2003) 30.

practice'.[26] Facilitating practices may be prohibited by section 5 of the *Federal Trade Commission Act* which prohibits unfair methods of competition in or affecting commerce.[27] A facilitating practice is condemned because it reduces uncertainty and has a tendency to increase the likelihood of tacit collusion.

According to one commentator, the hesitation on the part of businesses to report security intrusions stems from a number of factors, including fears of antitrust litigation:

> Industry has expressed concern that sharing information within a specific sector may prompt prosecution for violations of antitrust law. The Department of Justice has indicated that it will issue 'business review letters' to companies that are concerned about antitrust issues, offering assurances that it will not consider cybersecurity information sharing to be a violation of antitrust law. Industry representatives indicate that they find such assurances inadequate. Business review letters are not binding upon the Department of Justice. A change in the Executive Branch could bring a change in policy on this front. In order to avoid a stalemate that stymies national security progress, Congress needs to act quickly to provide assurance to private industry that information shared for purposes of protecting the economy and national security will not, in fact, constitute violation of the antitrust framework.[28]

It was the events of 9/11 which prompted Congress to specifically address perceived concerns that the antitrust laws could act as an impediment to an effective CIISS.

---

[26] See Phillip Areeda, *Antitrust Law*, vol 6, (Little Brown, Boston, 1986) para 1407b, who defines a facilitating practice as 'an activity that makes it easier for parties to coordinate price or other behaviour in an anticompetitive way'. See also Susan DeSanti and Ernest Nagata, 'Competitor Communications: Facilitating Practices or Invitations to Collude? An Application of Theories to Proposed Horizontal Agreements Submitted for Antitrust Review' (1994-95) 63 *Antitrust Law Journal* 93 and Kevin Arquit, 'The Boundaries of Horizontal Restraints: Facilitating Practices and Invitations to Collude' (1992-3) 61 *Antitrust Law Journal* 531.

[27] See *E I du Pont de Nemours & Co v FTC* 729 F 2d 128 (2nd Cir, 1984) (*The Ethyl Case*). The Court of Appeals upheld the FTC's authority to proscribe unilateral conduct in an oligopolistic industry as 'unfair' under s 5 of the *Federal Trade Commission Act*, but rejected the conclusion that the use of advance notice of price increases was likely to facilitate collusion. See George Hay, 'Facilitating Practices: The Ethyl Case (1984)', in John Kwoka and Lawrence White (eds), *The Antitrust Revolution: Economics, Competition, and Policy* (Oxford University Press, 3rd ed, 1999) 182.

[28] Emily Frye, 'The Tragedy of the Cyber-commons: Overcoming Fundamental Vulnerabilities to Critical Infrastructures in a Networked World' (2002) 58 *Business Lawyer* 349, 374–5.

1 Antitrust Exemption

On 24 September 2001 the Bennett-Kyl Bill, S 1456, 107th Congress, was introduced into the Senate and referred to the Senate Committee on Governmental Affairs. Hearings were held on 8 May 2002, chaired by Senator Joseph Lieberman.[29] In his testimony before the Senate Committee, Michehl R Gent, the President and Chief Executive Officer of the North American Electric Reliability Council stated:

> I am not an expert ... on antitrust law … but I have many years of practical experience in this industry. Based on that experience, I understand that company executives and managers believe they cannot prudently discuss certain matters with their competitors, suppliers, or customers. They believe that such discussions, and especially any resulting plans or actions, could be the source of antitrust litigation. In addition, even if a company might ultimately prevail, the great expense, potential risk of adverse publicity or even temporary loss, and possible public release of sensitive information during the course of such litigation lead them to not even begin the conversation in the first place. That diminishes our ability to improve our security in advance of a problem.
>
> These concerns go beyond the potential antitrust problems caused by merely sharing information about threats. In particular, entire industries are now having to address whether and how to share spare parts or other resources to repair major widespread damage and prevent worse calamities due to cascading failures. The issue of sharing also involves potential allocations of scarce commodities – both supplies for repair, and products for customers. Further, entire industries may determine security-related requirements to ask of their suppliers and business partners. At the least, entire industries may discuss the security-related short comings of existing products, suppliers and partners. Each of these actions is ripe for allegations of illegal market manipulation (boycotts, market allocations, etc).[30]

The purpose of the Bennett-Kyl Bill – S 1456, was to overcome these concerns and to encourage private entities to share information related to CI with the federal government. In that respect it contained an explicit antitrust exemption designed to facilitate such sharing. Clause 7 of the bill provided:

> (a) Antitrust Exemption – Except as provided in subsection (b), the antitrust laws shall not apply to conduct engaged in by an Information Sharing and analysis Organization or its members,

---

[29] Committee on Governmental Affairs, United States Senate, *Securing Our Infrastructure: Private/Public Information Sharing* (8 May 2002) <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_senate_hearings&docid=f:80597.pdf >.

[30] Ibid 91–2. See also the testimony of Harris N Miller, President of the Information Technology Association of America, at 102.

> including making and implementing an agreement, solely for the purposes of –
>
> (1) gathering and analysing critical infrastructure information in order to better understand security problems related to critical infrastructure and protected systems, and interdependencies of critical infrastructure and protected systems, in order to ensure the availability, integrity, and reliability of critical infrastructure and protected systems;
>
> (2) communicating or disclosing critical infrastructure information to help prevent, detect, mitigate, or recover from the effects of a problem related to critical infrastructure or protected systems; or
>
> (3) voluntarily disseminating critical infrastructure information to its members, other Information sharing and Analysis Organizations, State, local, or Federal Governments, or any entities that may be of assistance in carrying out the purposes specified in paragraphs (1) and (2).
>
> (b) Exception – Subsection (a) shall not apply with respect to conduct that involves or results in an agreement to boycott any person, to allocate a market, or to fix prices or output.

However, this specific exemption was not adopted in the *Critical Infrastructure Information Act, 2002* (US) (CII Act)[31] as part of the *Homeland Security Act 2002* (US). Rather, the CII Act provided for an indirect antitrust exemption via the *Defense Production Act of 1950* (DPA).[32] Pursuant to the DPA, Congress has given the President limited authority to shield agreements from antitrust laws.[33] The authority may only be used upon a finding of conditions that directly threaten the national defence or preparedness programs.

---

[31] Codified in 6 USC § §131-134 (2000).

[32] 6 USC §133(h) provides: 'The President may delegate authority to a critical infrastructure protection program, designated under section 132 of this title, to enter into a voluntary agreement to promote critical infrastructure security, including with any Information Sharing and Analysis Organization, or a plan of action as otherwise defined in section 2158 of title 50, Appendix.'

[33] 50 USC Appendix – War and National Defense § 2158. See Kristen Elizabeth Uhl, 'The Freedom of Information Act Post-9/11: Balancing the Public's Right to Know, Critical Infrastructure Protection, and Homeland Security' (2004) 53 *American University Law Review* 261, 278.

Paragraph 2158 (j) of Title 50, Appendix – War and National Defence provides:

> (1) In General
>
> Subject to paragraph (4), there shall be available a defence for any person to any civil or criminal action brought under the antitrust laws (or any similar law of any State) with respect to any action taken to develop or carry out any voluntary agreement or plan of action under this section that –
>
> (A) such action was taken –
>
> (i) in the course of developing a voluntary agreement initiated by the President or a plan of action adopted under any such agreement; or
>
> (ii) to carry out a voluntary agreement initiated by the President and approved in accordance with this section or a plan of action adopted under any such agreement, and
>
> (B) such person –
>
> (i) complied with the requirements of this section and any regulation prescribed under this section; and
>
> (ii) acted in accordance with the terms of the voluntary agreement or plan of action.
>
> …
>
> (4) Exception for Actions Taken to Violate the Antitrust Laws
>
> The defence established in paragraph (1) shall not be available if the person against whom it is asserted shows that the action was taken for the purpose of violating the antitrust laws.

The United States approach of relying on a specific legislated defence for the exchange of CI information clearly indicates that antitrust laws were viewed as an impediment to the operation of a CIISS. At the same time, the process was designed to ensure that the antitrust defence provided by the DPA was not abused. In this respect the defence is not available if the plaintiff is able to establish that the conduct at issue was a deliberate attempt to violate antitrust law.

B Australia: Trusted Information Sharing Network

In Australia, the Trusted Information Sharing Network for Critical Infrastructure Protection ('TISN') was launched by the Commonwealth in 2003 to provide a secure forum for owners and operators of CI and

government stakeholders to share information and discuss issues. The TISN resulted from a recommendation of the Business-Government Task Force on Critical Infrastructure which met throughout 2002.

The model adopted in Australia is very similar to the US model and relies on voluntary, industry self-regulation with little government intervention.

The information-sharing approach to CI protection aims to identify CI, analyse vulnerabilities, risks and sector interdependencies and prepare for 'hazards'.[34] The scheme requires active participation by owners and operators of CI in Australia. Given the inter-dependent nature of CI, effective protection is impossible without cooperation and coordination.[35]

The type of information envisaged to be shared includes:

- identification of 'critical' infrastructure;
- information regarding vulnerabilities of infrastructure;
- current risk management strategies;
- expected hazards including terrorism, cyber-attack, natural disaster etc;
- likely effects of different hazards;
- inter-dependencies of sectors and flow-on effects of attacks.[36]

By December 2007, nine Infrastructure Assurance Advisory Groups ('IAAGs') – the Australian equivalent of the ISACs – had been formed within the TISN scheme: Transport, Energy, Emergency Services, Banking and Finance, Health, Food Chain, Mass Public Gatherings, Water Services and Communications. Each IAAG is a closed community and comprises industry bodies such as councils and boards, industry participants who own, operate or use the specific critical infrastructure and relevant government departments. It is a closed community because it is dealing with sensitive and confidential information.

It seems that the information disclosed by the participants in the TISN falls into Category 1 and that the TISN has not yet evolved to deal with Category 2 information.

The Attorney-General's Department has established processes and procedures that must be followed when meetings are held. Each private sector participant

---

[34] Trusted Information Sharing Network, *About Critical Infrastructure Protection* <http://www.tisn.gov.au/www/tisn/tisn.nsf/Page/About_Critical_Infrastructure>.

[35] Ibid.

[36] Trusted Information Sharing Network, *Owners and Operators of Critical Infrastructure* <http://www.tisn.gov.au/www/tisn/tisn.nsf/Page/Stakeholders_Ownersandoperatorsofcriticalinfrastructure>.

in the TISN must sign a Deed of Confidentiality which 'is intended to facilitate information sharing within the TISN and assist companies to meet their existing legal obligations'.[37]

Members of each IAAG have access to the TISN website for their particular group which allows each member to know who the other members of the IAAG are and to exchange telephone numbers. Thus, for example, if the representative of a telecommunications company within the Communications IAAG becomes aware of some kind of cyber attack on the company, he or she can check with other members to see if they are experiencing the same or a similar sort of problem. The arrangements are quite informal and allow for a rapid response in relation to a perceived or actual threat.

The Critical Infrastructure Advisory Committee (CIAC) consisting of a representative of each IAAG co-ordinates communication between the sectors represented in the TISN and acts as a link with the Attorney-General who, in turn, is able to pass on any concerns to the Cabinet.

In relation to the risk of cyber attacks, the Australian Government Computer Emergency Readiness Team (GovCERT.au) was established in 2005 to assist in the formulation of e-security policy and to liaise with foreign government Computer Emergency Response Teams (CERTs).[38]

IV APPLICATION OF THE TPA TO TISN INFORMATION SHARING AND RELATED ACTIVITIES

In the same manner as their US counterparts, Australian private owners and operators of CI participating in the TISN scheme have raised concerns about the risk of contravening the TPA.[39] Accordingly, in this Part we examine first the way in which the new law might apply to TISN activities, and, secondly, the manner in which the new measures referred to earlier are likely to give rise to more serious concerns on the part of private sector owners and operators regarding the possible breaching of the TPA.

At one stage, the Commonwealth Attorney-General's Department considered seeking authorisation for the TISN scheme from the Australian Competition

---

[37] Trusted Information Sharing Network, *CIP Newsletter: Volume 4 Number 3 – Legal Issues* (October 2007) [6] <http://www.ag.gov.au/agd/WWW/rwpattach.nsf/VAP/(930C12A9101F61D43493D44C70E84EAA)~Legal+issues+final+final.pdf/$file/Legal+issues+final+final.pdf>.

[38] Australian Government Attorney-General's Department, *GovCERT.au* (24 November 2009) <http://www.ag.gov.au/govcert>.

[39] Trusted Information Sharing Network, above n 37, 4.

and Consumer Commission (ACCC).[40] Instead however, a discussion paper has been prepared which has been publicly endorsed by the Chairman of the ACCC.[41]

The most serious potential anti-competitive consequence of a CIISS could arise from Category 2 arrangements between horizontal competitors giving rise to an exclusionary provision.

A Application of Part IV, Division 1 of the TPA

The criminalisation of cartel conduct, provided for in the *Trade Practices Amendment (Cartel Conduct and Other Measures) Act 2009* (Cth) (CC & OM Act), which took effect on 24 July 2009, could operate in such a way as to constitute an impediment to the exchange of information that is necessary to protect CI from terrorist attack.

Division 1 contains two sets of prohibitions:

- The cartel offences under sections 44ZZRF and 4ZZRG; and
- The civil per se prohibitions under sections 44ZZRJ and 44ZZRK.

1 Cartel Offences

The main *cartel offence* is created by section 44ZZRF which provides:

> (1) A corporation commits an offence if:
>
> (a) the corporation makes a contract or arrangement, or arrives at an understanding; and
>
> (b) the contract, arrangement or understanding contains a cartel provision.
>
> (2) The fault element for paragraph (1)(b) is knowledge or belief.

Section 44ZZRG separately prohibits *giving effect* to a cartel provision in a contract, arrangement or understanding. The fault element is again knowledge or belief.

---

[40] Attorney-General's Department, *Information Sharing Arrangements* <http://www.ag.gov.au/agd/WWW/rwpattach.nsf/VAP/(930C12A9101F61D43493D44C70E84EAA)~info+sharing+presentation.ppt/$file/info+sharing+presentation.ppt>.

[41] Trusted Information Sharing Network, above n 37, 4.

The criminal offence in section 44ZZRF(1) comprises two physical elements:

- first, that the corporation makes a contract or arrangement or arrives at an understanding; and
- secondly, that the contract, arrangement or understanding contains a cartel provision.

In relation to the first physical element — the act of 'making a contract or arrangement, or arriving at an understanding' — there is no specified fault element. The default fault element is 'intention'.[42] For the purposes of the *Criminal Code* a person has the requisite 'intention' if '... he or she means to engage in that conduct'.[43]

In relation to the second physical element – the requirement that a contract, arrangement or understanding contain a cartel provision – the fault element specified in section 44ZZRF(2) is 'knowledge or belief'. Thus, in relation to the criminal offence in section 44ZZRF(1), it will be necessary to prove that an individual or corporation intended to enter into a contract, arrangement or understanding and that they knew or believed that the contract, arrangement or understanding contained a cartel provision.

The prosecution does not need to prove that the accused knew that the provision satisfied the definition of a cartel provision in section 44ZZRD, or that a cartel offence under section 44ZZRF(1) of making a contract arrangement or understanding containing a cartel provision has been committed.[44] It is only necessary for the accused to know that a provision 'possess[es] the qualities' that, by virtue of section 44ZZRD, go to make the provision a cartel provision, '... regardless of whether the accused appreciates the legal significance of those qualities'.[45] What is required is an awareness of the nature of the conduct defined in section 44ZZRD and prohibited in section 44ZZRF. A person has the requisite 'knowledge' of a circumstance or result if '... he or she is aware that it exists or will exist in the ordinary course of events'.[46] No additional element of dishonesty is required.

The TPA does not provide guidance as to whether cartel conduct should be pursued civilly or criminally. The matter is to be left to the ACCC in

---

[42] Explanatory Memorandum [2.30]. *Criminal Code Act 1995* (Cth) s 5.6 applies since creating a contract, arrangement or understanding is a form of conduct.

[43] *Criminal Code Act 1995* (Cth) s 5.2(1).

[44] See *R v Tang* (2008) 237 CLR 1 (*Tang Case*) and Alex Steel, 'What's to Know? The Proposed Cartel Offence' (2009) 32(1) *University of New South Wales Law Journal* 216.

[45] *Tang Case* (2008) 237 CLR 1 [48].

[46] *Criminal Code Act 1995* (Cth) s 5.3.

consultation with the Commonwealth Director of Public Prosecutions (CDPP). There are a number of differences between the cartel offence and the civil prohibition. In prosecuting the cartel offence it would be necessary for the CDPP to:

- establish the elements of each offence, including the fault element provided for in the *Criminal Code*;
- prove the offence beyond reasonable doubt; and
- obtain a unanimous verdict of the jury.

2 Civil Prohibitions

The new civil prohibitions in sections 44ZZRJ and 44ZZRK are in identical terms to the offences, except that they omit sub-section (2) relating to the fault elements.

The civil prohibitions require proof of three elements:

- a contract, arrangement or understanding;
- a cartel provision; and
- satisfaction by at least two of the parties to the contract, arrangement or understanding of the competition condition.

The first element – a contract arrangement or understanding – is considered below in relation to section 45(2) of the TPA.

As regards the second element, the concept of a cartel provision is central to both the criminal offences and the civil prohibitions in Part IV Division 1 and is defined separately for each. In order to satisfy the definition of a cartel provision in section 44ZZRD it is first necessary to establish that the provision at issue falls within one of the four different types of cartel provision in section 44ZZRD relating to –

- price fixing: section 44ZZRD(2);
- output restriction in the production or supply chain: section 44ZZRD(3)(a);
- market allocation (customers, suppliers or geographical areas): section 44ZZRD(3)(b); or

- bid-rigging: section 44ZZRD(3)(c).

The definitions are far-reaching. This is particularly so in relation to output restriction. Section 44ZZRD(3)(a) provides that a provision in a contract, arrangement or understanding is an output restriction provision if:

> … the provision has the purpose, of directly or indirectly:
>
> (a) preventing, restricting or limiting:
>
> (i) the production, or likely production, of goods by any or all of the parties to the contract, arrangement or understanding; or
>
> (ii) the capacity, or likely capacity, of any or all of the parties to the contract, arrangement or understanding; or
>
> (iii) the supply, of likely supply, of goods or services to persons or classes of persons by any or all of the parties to the contract, arrangement or understanding.

Section 44ZZRD(3)(a) prohibits provisions that have a direct or indirect purpose of reducing production, capacity or supply. It is not necessary to prove whether such reduction actually occurs or is likely to occur, and the extent of the reduction is likewise irrelevant.

The application of this definition of a cartel provision to a post-incident response-planning information-exchange arrangement is readily apparent. Consider the following examples.

Assume an attack on a number of electricity sub-stations that supply Sydney with much of its electricity. There are back-up supplies of diesel fuel to operate generators so that apartment dwellers can continue to live in their apartments until power is restored. An arrangement is entered into between fuel suppliers to ensure that back-up supplies of diesel fuel are rationed to ensure that the maximum number of apartment dwellers benefit. The purpose of the rationing provision is to restrict the supply of fuel to other users of diesel fuel such as motorists. The arrangement would be likely to fall within the definition of a cartel provision in section 44ZZRD(3)(a)(iii) despite the obvious public benefit of such a provision.

Assume that after the attack it is decided that private contractors will re-build the electricity sub-stations. The re-construction program contains a provision that requires the repair or rebuilding of the sub-stations to be given priority over less critical structures or facilities such as private dwellings. The subjective purpose of the parties is to allocate suppliers to certain tasks in

priority to other tasks. Such a provision is also likely to fall within the definition of a cartel provision in section 44ZZRD(3)(a)(iii).

As regards, the third element, section 44ZZRD(4) provides:

> The competition condition is satisfied if at least 2 of the parties to the contract, arrangement or understanding:
>
> (a) are or are likely to be, or
>
> (b) but for any contract, arrangement or understanding, would be or be likely to be;
>
> in competition with each other in relation to:
>
> …
>
> (d) if paragraph (2)(d) … applies in relation to an acquisition, or likely acquisition, of goods or services – the acquisition of those goods or services …

The final four words ('those goods or services') mean that at least two of the parties to the relevant contract, arrangement or understanding must be actual or potential competitors in relation to the goods or services that are the subject of the cartel provision, that is, the goods or services that are being acquired pursuant to the joint procurement collaboration.

3 Penalties for Contravening Cartel Offences and Civil Prohibitions

Both corporations and individuals can be made liable on two different bases. Primary liability attaches to corporations based on the conduct of an individual engaged in on behalf of the corporation.[47] Where a corporation is primarily liable for a cartel offence or a civil prohibition, an employee, servant or agent of the corporation may be liable as an accessory based on aiding, abetting, inducing, or being knowingly concerned in the offence or civil prohibition.

In relation to cartel offences the penalties that can be imposed are:

- for corporations, on conviction, a maximum fine that is the same as that for a civil contravention;[48]

[47] *Trade Practices Act 1974* (Cth) s 84(2).

[48] *Trade Practices Act 1974* (Cth) ss 44ZZRF(3) and 44ZZRG(3).

- for individuals, on conviction, a maximum fine of $220 000 and/or a maximum gaol term of 10 years.[49]

The penalties that can be imposed for breaches of the civil prohibitions are:

- for corporations, a maximum pecuniary penalty which is the greatest of $10 million, or three times the gain or 10 per cent of the annual turnover.[50]

- for individuals a maximum pecuniary penalty of $500 000.[51]

Given that the objective of the CC & OM Act is to strengthen deterrence, it is likely that the level of pecuniary penalties and fines imposed will increase under the new regime, and it is likely that the courts will impose custodial sentences in relation to cartel offences.

4 *Authorisation of Cartel Offences and Civil Prohibitions*

Section 88 provides that the ACCC may authorise conduct that would otherwise breach the prohibitions in Part IV. Section 88(1A) provides that the ACCC may authorise a corporation to make a contract, arrangement or understanding, or give effect to a contract, arrangement or understanding that contains a cartel provision. The tests to be applied in determining whether to give such an authorisation are set out in sections 90(5A) and (5B)

Section 44ZZRM provides that the cartel offences, sections 44RF and 44RJ, do not apply in relation to the making of a contract that contains a cartel provision if the contract is subject to a condition that the provision will not come into force unless and until the corporation is granted an authorisation, and the corporation applies for an authorisation within 14 days after the contract is made.

There are likely to be a number of provisions in contracts, arrangements and understandings that satisfy the definition of a cartel provision, but do not benefit from one of the exceptions. In that event the parties will be forced to seek authorisation from the ACCC.

---

[49] *Trade Practices Act 1974* (Cth) ss 44ZZRF(4) and 44ZZRG(4).

[50] *Trade Practices Act 1974* (Cth) s 76(1A).

[51] *Trade Practices Act 1974* (Cth) s 70(1)(e).

Section 177 provides that if an authorisation was granted prior to 24 July 2009 in relation to a cartel provision, the authorisation continues to apply in relation to the cartel provision.

B Application of Part IV, Division 2 of TPA

There is considerable scope for overlap between the cartel offences and civil prohibitions in Division 1 of Part IV, and the pre-existing prohibitions in section 45(2) of the TPA.

If a provision does not satisfy the definition of a 'cartel provision' in section 44ZZRD, it may satisfy the definition of an exclusionary provision in section 4D or be a provision that has the purpose, effect or likely effect of substantially lessening competition. In that case it would be prohibited by section 45(2).

Section 45(2) is the substantive prohibition which is of most relevance to a CIISS. It provides:

> (2) A corporation shall not –
>
> (a) make a contract or arrangement, or arrive at an understanding, if –
>
> (i) the proposed contract, arrangement or understanding contains an exclusionary provision; or
>
> (ii) a provision of the proposed contract, arrangement or understanding has the purpose, or would have or be likely to have the effect, of substantially lessening competition; or
>
> (b) give effect to a provision of a contract, arrangement or understanding, … if that provision –
>
> (i) is an exclusionary provision; or
>
> (ii) has the purpose, or has or is likely to have the effect, of substantially lessening competition.

Section 45(2) contains one per se prohibition in relation to contracts, arrangements or understandings that contain an exclusionary provision under section 45(2)(a) or (b)(i).

Section 45(2)(a) or (b)(ii) prohibits contracts, arrangements or understandings that contain a provision that has:

- the *purpose* of substantially lessening competition; or
- the *effect* of substantially lessening competition; or
- the *likely effect* of substantially lessening competition.

The prohibition in section 45(2) is not limited in its application to horizontal contracts, arrangements and understandings. It can also apply to vertical contracts that do not meet the definition of 'exclusive dealing' in section 47 of the TPA. This means that information-sharing between CIs operating at different functional levels of the market may also be caught.

Furthermore, the prohibition in section 45(2) does not require that the agreement be between competitors. This is only a requirement for per se prohibitions, namely the prohibition against exclusionary provisions as defined in section 4D of the TPA.

Sub-paragraph 45(2)(b) prohibits 'giving effect to'[52] provisions of contracts, arrangements or understandings which are exclusionary provisions or have the purpose or likely effect of substantially lessening competition.

In other words, contracts, arrangements and understandings containing provisions which are 'exclusionary provisions' are prohibited *per se*, but otherwise will fall within section 45(2) only if they have the *purpose* or *likely effect* of substantially lessening competition. An 'exclusionary provision' is defined in section 4D of the TPA but for present purposes is it sufficient to note that it must:

- be a provision of a contract, arrangement or understanding made (or proposed) between at least two competitors,[53] or persons who would be likely to be competitors if not for the exclusionary provision;[54] and
- have the purpose of preventing, restricting or limiting the supply or acquisition of goods or services to or from particular persons or classes of persons, by any or all parties to the contract.[55]

1 Exclusionary Provisions

Exclusionary provisions are likely to be found not just in arrangements which are clearly anti-competitive, such as those involving market allocation, but

[52] 'Give effect to', in this context, includes doing an act or thing in pursuance of or in accordance with or enforcing or purporting to enforce: *Trade Practices Act 1974* (Cth) s 4.

[53] *Trade Practices Act 1974* (Cth) s 4D(1)(a).

[54] *Trade Practices Act 1974* (Cth) s 4D(2).

[55] *Trade Practices Act 1974* (Cth) s 4D(1)(b).

also output restriction of a kind already considered in relation to the definition in section 44ZZRD(3)(a).

In the context of a CIISS, exclusionary provisions may arise from:

- agreements among competitors to allocate or ration supplies of spare parts for the repair of damaged CI;
- agreements among competitors to allocate scarce products among existing customers following an attack; and
- agreements among competitors to purchase only products that meet certain minimum security-related standards.

The wide-reaching effect of section 45(2) is illustrated by cases such as *Rural Press Ltd v ACCC*,[56] where an assurance given by a competitor that it would withdraw from a particular market was held to constitute a market sharing arrangement, even though it was extracted by threats. Counsel for Rural Press argued that it would be too 'draconian' to treat the market sharing arrangement at issue in that case as an exclusionary provision subject to per se treatment.

However, this was rejected by Gummow, Hayne and Heydon JJ[57] with whom Kirby J agreed.[58] Their Honours referred to the fact that market sharing arrangements are per se violations of the *Sherman Act* 1890 (US).

2 Contract, Arrangement or Understanding

Of course, not all collusive conduct is caught by section 45(2). It must be conduct pursuant to a 'contract, arrangement or understanding'. These terms are not defined in the TPA.

'Contract', in this context, has its ordinary common law meaning, ie, a transaction based on consensus which is enforceable at law.[59] By comparison, the words 'arrangement' and 'understanding' are intended to catch

[56] *Rural Press Ltd v ACCC* (2003) 216 CLR 53.

[57] Ibid 87-8. Their Honours referred to the fact that market sharing arrangements are per se violations of s 1 of the *Sherman Act 1890* (US).

[58] Ibid 98. See also *Visy Paper Pty Ltd v ACCC* (2003) 216 CLR 1, 13 (Gleeson CJ, McHugh, Gummow and Hayne JJ).

[59] *Hughes v Western Australian Cricket Association Inc* (1986) 19 FCR 10, 32.

transactions or dealings which are informal and may not give rise to a legally binding contract.[60]

Nonetheless, the arrangement or understanding, however informal, must evidence a consensus as to what is to be done reflecting some level of commitment, rather than a mere hope or expectation that the other party will behave in a certain way.

In the *CC (NSW)* case, Lindgren J summarised the current position:

> A mere expectation that as a matter of fact a party will act in a certain way is not enough, even if it has been engendered by that party. In the present case, for example, each individual who attended the Meeting may have expected that as a matter of fact the others would return to their respective offices by car, or, to express the matter differently, each may have been expected by the others to have acted in that way. Each may even have "aroused" that expectation by things he said at the Meeting. But these factual expectations do not found an "understanding" in the sense in which the word is used in ss 45 and 45A. The conjunction of the "understanding" with the words "agreement" and "arrangement" and the nature of the provisions show that something more is required.[61]

Lindgren J stated further: 'The cases require that at least one party "assume an obligation" or give an "assurance" or "undertaking" that it will act in a certain way'.[62] An understanding will usually, but not necessarily, involve some reciprocity of obligation.[63]

Only limited information about the operation of the Commonwealth's TISN is in the public domain. A fact sheet published by the Commonwealth Attorney-General's Department states:

> Participation in the TISN is voluntary and any information participants share is done so (sic) at their discretion. The [confidentiality] Deed specifically provides that there is no obligation on participants to disclose any information if they do not wish to do so.[64]

---

[60] *Trade Practices Commission v David Jones (Australia) Pty Ltd* (1986) 13 FCR 446, *ACCC v Leahy Petroleum Pty Ltd* (2004) 141 FCR 183, 54.

[61] *ACCC v CC (NSW) Pty Ltd* (1999) 92 FCR 375, 408.

[62] Ibid.

[63] *ACCC v Leahy Petroleum Ltd* (2004) 141 FCR 183, [54] (Merkel J).

[64] Trusted Information Sharing Network, *Fact Sheet: TISN Deed of Confidentiality* (October 2007) <http://www.tisn.gov.au/www/tisn/rwpattach.nsf/VAP/(E794A048FF84C896A06E1D7EC63DF5A4)~Fact+Sheet+-+TISN+Deed+of+Confidentiality.pdf/$file/Fact+Sheet+-+TISN+Deed+of+Confidentiality.pdf>.

This appears to rule out the existence of a legal obligation upon TISN participants to share any relevant information. Nonetheless, participants may feel morally bound to share such information with the TISN as good and responsible corporate citizens, acting in the interests of the national security. To the extent that there is some objective evidence of a mutually felt obligation of this nature, this may amount to a sufficient level of 'commitment' to constitute an arrangement or understanding for the purposes of section 45(2) of the TPA.[65]

Moreover, an arrangement or understanding of the kind envisaged by section 45(2) of the TPA would also be possible, even though there was evidence that one or more TISN participants did not freely participate in the sharing of the relevant information in the sense that their participation was in some degree coerced or the result of outside pressure.

For instance, if it could be established that a TISN participant 'volunteered' information based on the belief that, if it did not do so, the Commonwealth would legislate to compel disclosure, this may be sufficient to constitute an arrangement for the purposes of section 45(2).[66] On the other hand, a mere hope or expectation that others will share information would not be sufficient.[67]

For example, in *Australian Competition and Consumer Commission v Leahy Petroleum Pty Ltd*,[68] the evidence established that petrol stations had been telephoning each other to give advance notice of proposed price changes, and inquiring whether the other party would follow suit.[69] However, a contravention of section 45(2) was not established. This was because there was no evidence that the parties to the alleged arrangement or understanding felt bound to follow the suggested price changes. Although there was evidence that in many cases the price changes were followed, there was also evidence that, in many cases, the proposed changes were not followed.

---

[65] See generally *Top Performance Motors Pty Ltd v Ira Berk (Qld) Pty Ltd* (1975) 5 ALR 465, 469–70.

[66] See, eg, *Rural Press Ltd v ACCC* (2003) 216 CLR 53.

[67] *Stationers Supply Pty Ltd v Victorian Authorised Newsagents Association Ltd* (1993) 44 FCR 35, 61, approved by the Full Court in *News Ltd v Australian Rugby Football League Limited* (1996) 64 FCR 410, 571-2.

[68] *ACCC v Leahy Petroleum Pty Ltd* (2007) 160 FCR 321.

[69] See, eg, *ACCC v Leahy Petroleum Pty Ltd* (2007) 160 FCR 321, 931. See Ian Tonking, 'Belling the CAU: Finding a Substitute for "Understandings" about Price' (2008) 16(1) *Competition and Consumer Law Journal* 46 and Ian Wylie, 'Understanding Understandings under the Trade Practices Act – An Enforcement Abyss' (2008) 16 *Trade Practices Law Journal* 20.

This indicates that it would be difficult to establish a contravention of section 45(2) in a CIISS environment. Even if it could be established that competitors in a CIISS environment were sharing information about relevant matters, it would not necessarily follow that a contravention of section 45(2) had occurred. In particular, there would need to be evidence of 1) a consensus or meeting of minds or some level of commitment by at least one of the participants in the CIISS as to how to implement a recovery plan after an attack on CI, and 2) which participant will be responsible for supplying particular geographical locations or particular customers.

3 Information-Sharing: Likely Effect of Substantially Lessening Competition

Information-sharing may be essential to enable competitors to share a common CI facility such as a transport network (airlines sharing a common airport, trains sharing the same rail track), or an energy network (power generators sharing the same electricity grid, gas producers sharing the same gas pipeline). Such information-sharing is essential for the proper functioning of the CI network.[70] Information-sharing of this kind will not have the purpose, effect or likely effect of lessening competition. In network industries, co-operation may be necessary to facilitate competition and promote efficiency.

However, in some situations information-sharing can lessen competitive rivalry – for instance, in oligopolistic markets for homogeneous products. This is because competition in an oligopolistic industry depends on firms having some measure of uncertainty as to the actions of their competitors.

A number of CI industries participating in the TISN share these characteristics. For example, within the Energy IAAG there are only a small number of natural gas producers and a small number of electricity generators. Moreover, within these Groups there might be concerns if firm specific transaction data for each competitor were to be disclosed to the other participants in the TISN; or if participants were to discuss future plans rather than disseminating data relating to past transactions.

In other words, the use of a TISN to share confidential information which is not publicly available may remove some of the uncertainty that would otherwise prevail, leading to parallelism of prices and other terms and conditions of sale or product offerings. Whether this would be sufficient to

[70] Dennis Carlton and J Klamer, 'The Need for Coordination among Firms, with Special Reference to Network Industries' (1983) 50 *University of Chicago Law Review* 446.

constitute a substantial lessening of competition would depend on the structure of the particular market.

Sharing information about product characteristics can facilitate product standardisation. Product standardisation can be used to enable a competitor to ascertain the price of another competitor's product. Information about the quality and contents of a competitor's product allows an assessment of that competitor's costs of production, and the price which that competitor is likely to charge in the market. Thus, while sharing product quality information poses less of a risk than sharing price information, it may have the effect or likely effect of producing price uniformity, or less vigorous price competition.

Section 45(2) of the TPA catches arrangements or understandings that have the effect or likely effect of substantially lessening competition.[71] In other words, an arrangement or understanding between competitors whose purpose is completely innocent, such as mitigating the consequences of a terrorist attack, will nevertheless contravene section 45(2) if its *likely effect* is to substantially lessen competition.

In this context the word 'substantially' does not set a very high threshold. In *Rural Press Ltd v ACCC* Gummow, Hayne and Heydon JJ (with whom Gleeson CJ and Callinan J agreed) stated that the word 'substantial' was used 'in the sense of being meaningful or relevant to the competitive process'.[72]

This then poses two questions: first, could a CIISS be an 'arrangement or understanding' within the meaning of section 45, and secondly, if so, could the operation of the CIISS be regarded as having the likely effect of substantially lessening competition?

Competition is synonymous with independent rivalry or striving to produce the goods and services that are most highly valued by consumers at the lowest price and at the highest quality. This presupposes independent decision-making as regards the price-quality-service package that is offered to consumers. The competitive process necessarily involves an element of uncertainty and risk, in part caused by limited information as to the capabilities, capacity, intentions and activities of competitors, customers, and suppliers. The sharing of this information pursuant to a CIISS may tend to lessen this uncertainty and have a chilling effect on competition in those markets where there is only a small number of competitors.

---

[71] *Trade Practices Act 1974* (Cth) s 45(2)(a)(ii) and 45(2)(b)(ii).

[72] *Rural Press Ltd v ACCC* (2003) 216 CLR 53, 71.

Firms compete, not just on price, but in other dimensions as well, including the features of their products and the level of service they provide to their customers. In so far as information-sharing pursuant to a CIISS results in the disclosure of vulnerabilities and solutions it will result in uniformity across the sector, with some firms giving up their competitive advantages for the greater good of protecting national security. While this may be a laudable motive, it will not take the conduct outside the ambit of section 45(2). Exchanging information about product quality can lead to product standardisation which, in turn, can facilitate anti-competitive price uniformity where there are only a small number of competitors in a market.

V INCREASED UNCERTAINTY: PROPOSED NEW MEASURE

A proposed new measure canvassed by the Discussion Paper released on 8 January 2009 by the Assistant Treasurer and Minister for Competition Policy and Consumer Affairs may, if it is adopted, increase the risk of contravening Divisions 1 and 2 of Part IV of the TPA and act as a further disincentive to participating in a CIISS.[73]

By way of background, the ACCC had in 2007 complained that the Federal Court's interpretation of what constitutes an illegal 'understanding' for the purposes of section 45(2) has made it too difficult to prove that competitors have colluded. This led to its proposing a new way of approaching the term 'understanding'.

In its *Petrol Report*,[74] the ACCC expressed the view that cases such as *Leahy Petroleum* have narrowed the scope of conduct caught by the term 'understanding' as used in section 45(2) because of the need to prove a 'commitment'. The ACCC recommended that the TPA be amended to broaden and clarify the meaning of the term 'understanding'. The ACCC recommended that consideration be given to amending the TPA to provide for an expanded definition of 'understanding' as follows:

> (a) The court may determine that a corporation has arrived at an understanding notwithstanding that:

---

[73] Australian Government, The Treasury, *Discussion Paper – Meaning of 'Understanding' in the Trade Practices Act 1974* <http://www.treasury.gov.au/contentitem.asp?NavId=037&ContentID=1459> .

[74] Australian Competition and Consumer Competition, *Petrol prices and Australian consumers: Report of the ACCC inquiry into the price of unleaded petrol* (December 2007) <http://www.accc.gov.au/content/item.phtml?itemId=806216&nodeId=d5fc6a56fb589b453abc58f22e0b78bd&fn=Petrol%20prices%20and%20Australian%20consumers%20all%20chapters.pdf >.

(i) the understanding is ascertainable only by inference from any factual matters the court considers appropriate

(ii) the corporation, or any other parties to the alleged understanding, are not committed to giving effect to the understanding.

(b) The factual matters the court may consider in determining whether a corporation has arrived at an understanding include but are not limited to:

(i) the conduct of the corporation or of any other person, including other parties to the alleged understanding

(ii) the extent to which one party intentionally aroused in other parties an expectation that the first party would act in a particular way in relation to the subject of the alleged understanding

(iii) the extent to which the corporation was acting in concert with others in relation to the subject matter of the alleged understanding

(iv) any dealings between the corporation and any other parties to the alleged understanding before the time at which the understanding is alleged to have been arrived at

(v) the provision by the corporation to a competitor, or the receipt by the corporation from a competitor, of information concerning the price at which or conditions on which, goods or services are supplied or acquired, or are to be supplied or acquired, by any of the parties to the alleged understanding or by any bodies corporate that are related to any of them, in competition with each other

(vi) whether the information referred to in (v) above is also provided to the market generally at the same time

(vii) the characteristics of the market

(viii) the likelihood of the information referred to in (v) above being useful to the recipient of the information for any purpose other than fixing or maintaining prices;

(ix) the extent to which, if at all, the communication referred to in (v) above was secret or intended by the parties to the communication to be secret.[75]

The ACCC proposal is designed to overcome the problem of proving the element of commitment when nothing has been reduced to writing. The

[75] Ibid 230.

proposed new methodology would remove the need for any level of commitment, and clarify that a court may find that a corporation has arrived at an understanding by inference from the surrounding facts without the need for direct evidence.

In his response to the ACCC reform proposal, the Assistant Treasurer and Minister for Competition Policy and Consumer Affairs, the Hon Chris Bowen MP, released the abovementioned Discussion Paper on the meaning of 'understanding' in the TPA.[76]

If the Government were to adopt the ACCC's recommendation this could act as a significant disincentive to private sector operators participating in the TISN.

VI POSSIBLE APPROACHES FOR SHIELDING PRIVATE SECTOR PARTICIPANTS IN THE TISN

Bearing in mind the manner in which the matters discussed above could impede the effective operation of a CIISS like the TISN, it is now appropriate to consider the possibility of some form of immunity for TISN related activities.

There are three possible approaches by which immunity from contravening the TPA could be conferred on the private sector participants in the TISN:

1. authorisation under the TPA;

2. exemption conferred under special purpose Commonwealth legislation; and

3. amendments to the TPA.

A Authorisation

The process of receiving authorisation under section 88 of the TPA is available to applicants so that they can obtain immunity and avoid contravening section 45(2). It is a protracted process that requires the applicant to specify in advance the conduct in question, and the public detriments (including any lessening of competition) likely to flow from it, as well as the public benefits.

[76] Australian Government, above n 70.

The ACCC is then required to consult with industry. Once the ACCC has considered the application, it issues a draft determination and provides an opportunity for industry players to request a conference. Following any such conference, the ACCC will reconsider the application and issue its final determination.

An authorisation will only confer immunity for the conduct as described in the application for authorisation. However, while reducing the risk of a terrorist attack would constitute a clear public benefit, the problem with the authorisation procedure is that a CIISS, like the TISN, is constantly evolving over time to deal with new threats as they emerge. The problems are prospective. Some may be hypothetical. They do not lend themselves to being described in advance.

B Special Purpose Legislation

A second mechanism for obtaining immunity and avoiding a contravention of the substantive prohibitions of the TPA is for the Commonwealth Parliament to pass separate legislation that grants an exemption. Section 51(1)(a) of the TPA provides that, in deciding whether a person has contravened Part IV, anything specified in and specifically authorised by any other Commonwealth Act (other than an Act relating to patents, trade marks, designs or copyright) or regulations made under such an Act, must be disregarded.

Section 51(1)(a) is subject to the limitation in section 51(1C)(a) which provides that the authorising provision must specifically refer to the TPA.

C Amendments to the TPA

The third mechanism for removing liability under the TPA is to amend the TPA itself to provide for a specific defence for any person to any civil or criminal action brought under the TPA with respect to information-sharing under an IAAG or any plan of action relating to a terrorist threat or attack. The defence would be available provided the information-sharing was not undertaken for the purpose of contravening a competition provision of the TPA.

VII CONCLUSION

As stated earlier, there is broad agreement with regard to the strong policy against anti-competitive practices enshrined in Part IV of the TPA. However, it is also recognised that protecting competition must give way to other policy

objectives that have a more pressing claim, such as physical security from the threat of terrorist attack.

The first challenge for a CIISS like the TISN is to get IAAG members to share information. If the arrangement is to operate effectively, private sector operators of critical infrastructure must be encouraged to share information about vulnerabilities, threats, intrusions and possible solutions amongst themselves in a full and frank manner – and also to share this information with the government, so that it can issue warnings and take appropriate action. It is difficult enough to get business entities to share such sensitive and confidential information in the normal course of things, without the added risk that doing so may involve a contravention of the TPA.

In the United States, the Cyberspace Policy Review recognised that the existing public-private partnerships '... have fostered information sharing and served as a foundation for U.S. critical infrastructure protection and cyber-security policy for over a decade.'[77] However, it also recognised that there is an urgent need to develop response and recovery plans and to conduct a national dialogue on cyber-security. The United States is already moving away from voluntary regulation to the adoption of mandatory standards in the energy and chemicals sectors.

The Cyberspace Policy Review recognised that federal laws in the United States, including the antitrust laws, were impeding full collaborative partnerships and information-sharing between the private sector and government. While recognising that 'antitrust laws provide important safeguards against unfair competition'[78] the report recognised the need for government to '... work creatively and collaboratively with the private sector to identify tailored solutions that take into account both the need to exchange information and protect public and private interests and take an integrated approach to national and economic security'.[79]

The existing TISN type of CIISS in Australia has been operating since 2003, with the participation of Commonwealth government agencies. At this stage it appears to be limited to Category 1 information disclosure. As yet there has been no application for authorisation under the TPA, and there has been no indication of any move towards enacting a specific exemption or statutory defence to protect the current TISN information-sharing arrangements. In fact, it has been reported officially that:

---

[77] White House, above n 6, 18.

[78] Ibid 19.

[79] Ibid.

> Advice to date is that general discussions within the TISN are not likely to raise issues relating to the competitiveness in the market place as they are generally in relation to security policies, threats and vulnerabilities. A similar view is taken of TISN meetings, at which government officials are present, as they are not a forum for detailed price and market information to be shared between competitors. Where representatives do wish to discuss information that could result in reaching some sort of agreement, it may be appropriate to seek authorisation from the Australian Competition and Consumer Commission (ACCC). The Attorney-General's Department has prepared a paper on this issue endorsed by the Chairman of the ACCC, Mr Graeme Samuel.[80]

Because of the secrecy surrounding TISN meetings it is not possible to ascertain how many private owners and operators of critical infrastructure participate in the information exchange; what kinds of officials represent the owners and operators at the meetings; what kinds of information are disclosed; or how extensive is the level of disclosure, especially in relation to breaches of cyber-security.

Some kinds of Category 1 information-exchange (pertaining to risk minimisation prior to a terrorist attack) may have unintended anti-competitive consequences. For example, where private operators of CI compete with each other, the exchange of information about the reliability of their respective services, or vulnerability to attack could lessen competitive rivalry. While there may be no legal impediments to the exchange of *security-related* information, the exchange of commercially sensitive information and confidential know-how about how infrastructure and technology operates and how to make it more reliable, may have unintended anti-competitive consequences.

Category 2 information-exchange (pertaining to incident response and recovery plans) involves a more serious risk of contravening Divisions 1 and 2 of Part IV of the TPA. Where CIISS participants stop competing with each other to implement recovery plans, they are likely to agree to restrict supply to certain persons or classes of persons. In particular, whenever competitors come together for a joint project, for instance as a consortium to implement a recovery plan after a terrorist attack on CI, or for the purpose of deciding in advance which participants will be responsible for supplying particular geographical locations or particular customers, this conduct will be caught by section 44ZZRD (3)(a)(iii) and section 4D.

The exchange of information concerning current and future production capacity can also lessen competition. Clearly, a firm's estimate of its own

[80] Trusted Information Sharing Network, above n 37, 4.

future capacity is likely to be modified in the light of what it learns of the plans of others. The exchange of such information thus preserves existing market shares, removes potential competition, and reduces the choice of sources of supply.

The risk of contravening Divisions 1 and 2 of Part IV of the TPA is a legal impediment to private sector owners and operators of CI participating fully in TISN activities. The enactment of a special statutory defence under the TPA is necessary to shield these arrangements from competition law and would send a clear signal from the government that such information-sharing activities are not only permissible, but are to be actively encouraged.

The Federal government in Australia needs to turn its mind to developing a solution for Australia similar to that adopted in the United States.