Australian Government
Australian Institute of Criminology

Trends & issues in crime and criminal justice

ISSN 0817-8542

No. 566 December 2018

Abstract | Criminal intelligence has become a central tool in modern crime control that is used by law enforcement to understand rapid changes in crime and criminality. The development of intelligence relies on the sharing of information between agencies—including law enforcement, other government agencies and private sector entities.

However, there are a number of legislative, technical and cultural barriers that limit the free flow of information. This report examines those barriers and develops an information sharing matrix that explains the barriers associated with different types of information sharing.

The matrix develops a typology of information sharing based on two dimensions: the level of interaction and the level of connectivity.

Understanding law enforcement information sharing for criminal intelligence purposes

Rick Brown

Criminal intelligence has become a central tool to support modern crime control (Ratcliffe 2016; Rickards 2016). Law enforcement efforts have focused on improving criminal intelligence to understand the nature and extent of criminality and ultimately to prevent, detect and disrupt crime. Such criminal intelligence relies on the building blocks of raw data and information generated internally by a law enforcement agency or shared by a partner. In a world characterised by increasingly sophisticated crime, it is increasingly important to draw together the fragments of information available from multiple sources. As Bigo (2000: 84) has noted: 'A large amount of police work now concerns patrolling the data in order to spot connections between criminals, and much of this goes beyond the merely local or even national.' This might include 'patrolling' information from (among others) law enforcement agencies, intelligence agencies, government departments, financial institutions and telecommunications providers, each of which may provide a different insight into the activities of a criminal group.

This paper explores some of the ways in which information is shared between law enforcement agencies to help create actionable criminal intelligence. It addresses the benefits of and barriers to effective information sharing and outlines a way of assessing the maturity of information sharing arrangements.

Terminology

As a starting point, it is important to define what is meant by information and intelligence and to clarify how the two are different. Although there is no nationally agreed definition of criminal intelligence in Australia, it is defined here as 'information that is collected about crime and criminals and evaluated, analysed and disseminated' (Parliamentary Joint Committee on Law Enforcement 2013: 5). *Information* is the raw material used to create intelligence. This can come in many forms including unprocessed data (eg telecommunications metadata), details of criminal records, or information reports entered into a law enforcement intelligence database (eg a sighting of an individual at a particular location). Information may also include material processed by another law enforcement agency to produce a knowledge product that provides further understanding about a particular type of criminality or criminal group. Information, often from multiple sources, is collated and analysed to provide intelligence, which is typically actionable and intended to influence decision making about how to tackle crime or criminals. While Ratcliffe (2016) describes data, information, knowledge and intelligence as being on a continuum, the first three are characterised here as building blocks for the latter.

In this paper, information sharing is discussed in the context of law enforcement. It may also include sharing with those working in a national security or private sector setting, but this is not an essential requirement. Further, information may be shared without an immediate intent but rather for some future unknown requirement, it may be shared in support of a specific operation or investigation, or it may be shared in response to an urgent request.

Benefits of information sharing

Sharing information to improve criminal intelligence serves first and foremost to increase knowledge available for decision making. This can help not only to identify which criminal groups to target, but also, in an age of resource constraints, to triage out lower risk cases (Ratcliffe 2016). It can also help to prevent 'linkage blindness', where information available in one jurisdiction is not available in other jurisdictions. This can result in the full extent of criminality that transcends law enforcement boundaries remaining hidden (Jackson & Brown 2007; Sheptycki 2004). Linkage blindness was a problem identified by the 9/11 Commission in the United States, which found that a number of intelligence agencies held information on the activities of those involved but failed to connect the dots (National Commission on Terrorist Attacks Upon the United States 2004). Similarly, in the United Kingdom the Bichard inquiry into the murder of two children by a school caretaker identified failings in intelligence sharing between police forces and child protection services resulting in linkage blindness. The report of the inquiry recommended the implementation of a national police intelligence system as a matter of urgency (Bichard 2004). In each case, improved information sharing between jurisdictions could have resulted in an enhanced intelligence picture.

Information sharing also helps to support deconfliction (Mapel 2014; Police Foundation 2016), which aims to prevent what might be considered the opposite of linkage blindness—when more than one law enforcement agency is simultaneously investigating the same individual or group. Information sharing under these circumstances can result in savings in time and resources for each agency concerned by preventing duplication of effort (Parliamentary Joint Committee on Law Enforcement 2013). This is pertinent in Australia, where criminal intelligence on an entity may be held in multiple databases. A 2013 parliamentary inquiry into Australian criminal intelligence found that such information might be held on more than 30 separate systems operated by multiple law enforcement, policing and government agencies (Parliamentary Joint Committee on Law Enforcement 2013).

Law enforcement information sharing can also result in greater outcomes than would be possible for a single agency working alone. For example, in the context of drug law enforcement investigations instigated by the US Drug Enforcement Administration, Lemieux (2010) found a positive correlation between the number of police agencies involved and the average size of a drug seizure. Further, investigations involving multiple overseas law enforcement agencies tended to result in significantly more arrests and greater seizures than solo investigations.

Risks of information sharing

While there are clear benefits to information sharing, there are also risks. Maintaining and transmitting information securely is a significant task for law enforcement agencies. It requires trusting that recipient agencies handle and share their information securely. This means that those operating within an information sharing network are expected to abide by a common set of security standards governing the storage and dissemination of information. Sheptycki (2017) has noted that this may demarcate 'insiders'—those with whom the police will share information—from 'outsiders', with whom they will not. This can be particularly pertinent when dealing with some foreign jurisdictions, where trust may be eroded by high levels of public sector corruption.

Yet even within a trusted environment there can be information leakage from internal sources (eg corrupt employees), or external sources (eg data theft resulting from hacking). This can reduce the level of trust that other members of the network have in those subject to leaks, which in turn may impede information flows. As a result, there is a constant trade-off between the need to share information and the need to ensure that, when it is shared, it is held securely.

Barriers to effective information sharing

While significant benefits can be derived from information sharing, there remain a number of barriers that prevent information from being shared with others who might use it to generate intelligence. These can be divided into legislative, cultural and technological barriers.

Legislative barriers

Across Australia, there is no agreed legal definition of criminal intelligence among the eight states and territories and the Commonwealth (Parliamentary Joint Committee on Law Enforcement 2013). Rickards (2016) noted that each Australian state and territory has its own legislative framework governing information sharing between agencies, with a further set of frameworks to negotiate at the Commonwealth level. One example of Commonwealth information sharing restrictions can be found in section 59 of the *Australian Crime Commission Act 2002*, which places strict limits on whom the Australian Criminal Intelligence Commission (ACIC) can share information with, due to concerns over the security and privacy of that information. For example, telecommunications intercept material can only be shared with a small number of specified entities. Further, telecommunications companies may provide details of the same subscriber's phone records to multiple law enforcement agencies under separate dissemination processes due to different laws in each state/territory and the Commonwealth. Each agency receiving the information may be unaware that others have also requested and received it under their own legal powers, thereby creating inefficiencies (Parliamentary Joint Committee on Law Enforcement 2013).

In the context of terrorist events, the inquest in the wake of the Lindt Café siege raised questions about the limits placed on information sharing by privacy legislation and recommended a review of information sharing arrangements between agencies during terrorist events (State Coroner of New South Wales 2017).

Cultural barriers

Creating a culture of information sharing has previously been identified as a critical success factor in implementing an Australian criminal intelligence management strategy (Commonwealth of Australia 2017). Here, 'culture' is defined as the rituals, values and behaviours (Schein 2017) of the overall criminal intelligence community (rather than its constituent parts) that give rise to the overall framework that shapes the willingness of individual entities to share information. The literature on this issue has identified significant cultural barriers that can inhibit the flow of information between agencies. Some of these relate to the organisational structures that shape the operating environment, such as by creating silos. Organisations, and indeed sections or teams within organisations, often gain specialist knowledge about particular crime problems or criminal groups as a result of investing resources or using designated legal powers to target issues of concern to the agency. There can be a tendency to focus internally on building intelligence holdings, rather than cooperating with other agencies (Sales 2010). This can create a network of siloed intelligence holdings (also known as 'stovepipes') and reduce opportunities for information from multiple sources to be synthesised (Occhipinti 2010).

Many cultural attitudes to information sharing are a result of relational properties that determine how agencies interact (Whelan 2016). These include:

- ego—an agency can develop an ego that seeks to control. Intelligence can act like a currency, with power derived from sharing, trading or withholding information. Organisations may be inhibited from sharing information if they believe there will be additional gain from holding onto that information (Carter & Carter 2009). Ego can also lead to conflict between law enforcement agencies over who should take the credit for successful outcomes in multi-jurisdictional investigations (Guille 2010; Lemieux 2010);
- competition—organisational concern with sharing credit may extend to direct competition with other law enforcement agencies over achieving positive outcomes. If sharing information is expected to enhance the reputation of another agency, which could ultimately result in additional resources for that agency, a decision may be made to withhold the information (Aviram & Tor 2003; Jackson & Brown 2007; Sales 2010);
- filtering—agencies may filter the information they provide to others, thereby providing only some of that which is available (Jackson 2014);
- distrust—agencies may not provide information because they distrust the recipient agency. This can be due to concerns over whether the information will be held securely, or how it will be used (Monahan & Palmer 2009);
- mutuality—information sharing may be inhibited in circumstances where a degree of reciprocity is expected. An agency may provide information on the expectation that it will receive something in return, whether that be information, intelligence or recognition of the contribution made by that agency to any subsequent successful outcome. Failure to reciprocate can lead to a 'once bitten, twice shy' mentality (Sales 2010);
- competence—information may not be shared because it raises embarrassing questions about the quality of the information, in terms of its accuracy, its timeliness, or the method by which it was obtained (Jackson & Brown 2007; Taylor & Russell 2012);
- need-to-know—there may be a culture of not sharing information widely because of a belief in a need-to-know policy, as opposed to a need-to-share policy (Carter & Carter 2009; National Commission on Terrorist Attacks Upon the United States 2004). This means that an agency may judge whether its information has utility for another agency, rather than the recipient agency having an opportunity to evaluate that information for itself; and
- culture of secrecy—associated with the need-to-know ethos, there may be a general fear of sensitive information that could do harm to society getting into the wrong hands, leading to a non-sharing default position (Connery 2016).

Technological barriers

Technological problems have long plagued law enforcement agencies' attempts to share information. Incompatible IT systems that inhibit the transfer of information between entities have posed significant problems (Jackson & Brown 2007; Monahan & Palmer 2009; Plecas et al. 2011; Rickards 2016). In Australia, each of the eight states and territories has its own IT infrastructure for managing criminal intelligence, with systems that evolved at different times, with different operating systems. This has resulted in there being '…no single and complete "point-of-truth" for Australian criminal intelligence holdings nor an automated process for searching across all such systems simultaneously' (Parliamentary Joint Committee on Law Enforcement 2013: 38).

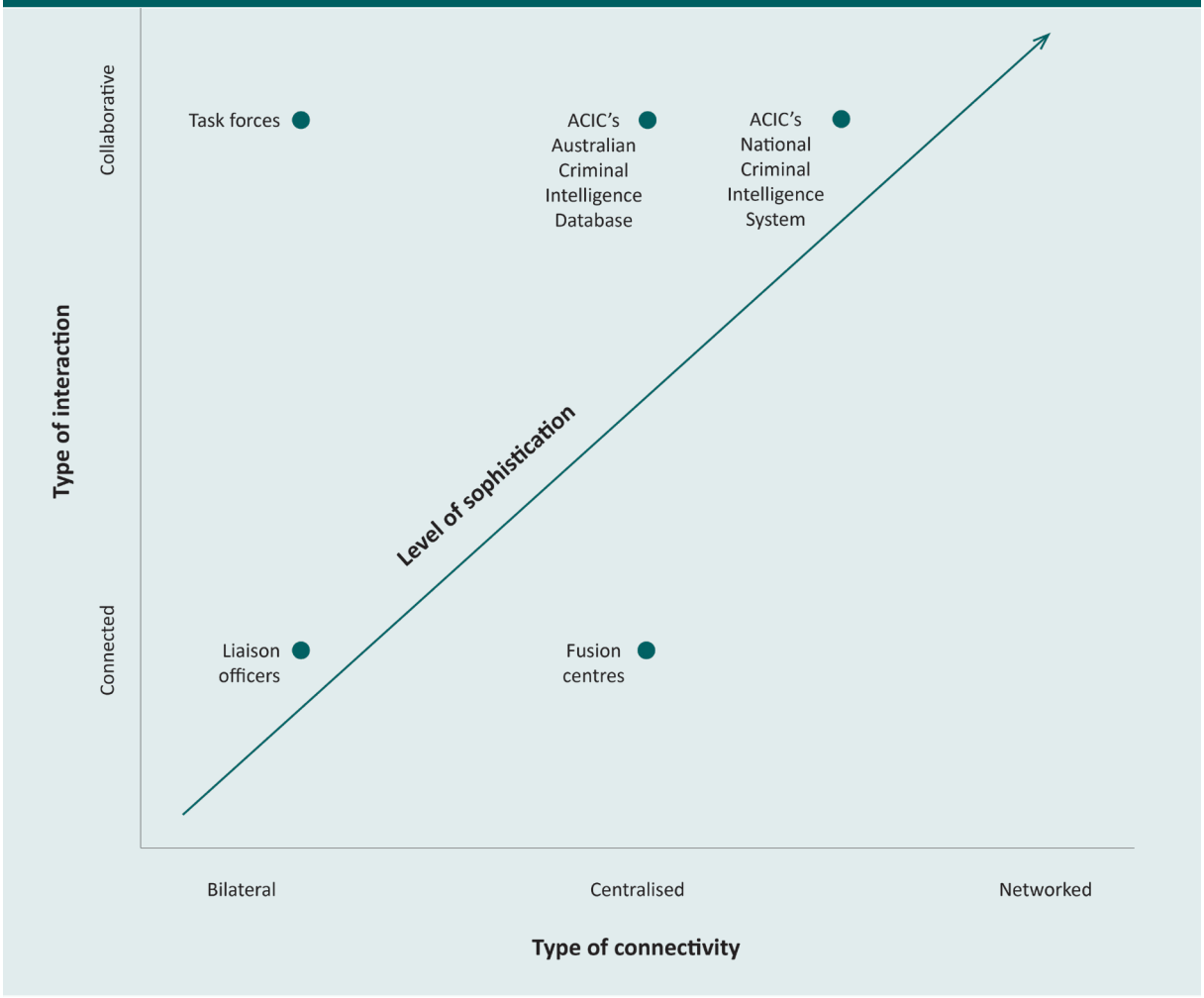
Other technical issues can also inhibit sharing. For example, differences in the way that names and other details are captured can mean that links between systems are missed, or duplicate records created when matching data between systems (Plecas et al. 2011).

Modes of information sharing

Despite the benefits of information sharing noted earlier, it remains deceptively difficult to achieve as a routine way of doing business. So what can be done to improve the way in which law enforcement agencies share information in a secure and mutually beneficial way? One small first step to answering this question is to understand the different approaches to sharing information and to recognise their inherent strengths and weaknesses. Indeed, there are multiple forms of sharing, some of which are context dependent and not all of which achieve the same outcome. The remainder of this paper therefore seeks to develop a typology of information sharing which can be used to assess the sophistication of information sharing processes within a law enforcement environment. Sophistication is determined here by the ease with which information is shared and the complexity of establishing the information sharing system. This assumes there is a hierarchy of intelligence sharing approaches with, by definition, some forms of sharing being superior to others. This is not to suggest that all information sharing should seek to achieve the same standard, but rather to acknowledge that decisions made about how information is shared shape subsequent approaches to working with that information.

Figure 1 introduces a prototype information sharing matrix. This takes into account the type of interaction and type of connectivity involved in the information sharing process. Movement along either axis in the matrix represents an increase in the sophistication of information sharing. In this context, 'interaction' relates to how the provider and the recipient of the information relate to each other. This can range from no interaction beyond the transmission of the information through to regular, direct interaction. Connectivity refers largely to the method of sharing.

Figure 1: Information sharing matrix



Type of interaction

The inclusion of interaction in Figure 1 is recognition that information sharing is a means to an end that is defined by the provision of better intelligence. At some point, there needs to be a degree of processing applied to the information before it can inform decision making. The term 'interaction' therefore situates information processing at the time the information is shared or at some later point. In the information sharing matrix, interactions are described as either connected or collaborative, although these should be considered as opposite ends of a continuum, rather than discrete categories.

Connected interaction

Connected interactions involve the delivery of intelligence from one law enforcement agency to another. This may be associated with a 'push' approach to information sharing whereby one agency passes information to another agency, or a 'pull' approach where information is requested (Jackson 2014). However, a key feature of connected interactions is limited communication between entities beyond the sharing of information. This communication may include limited context about how or why the information was collected or requested and there may be limited joint activity between the two entities beyond the information sharing. Examples include law enforcement officers entering information reports into a centralised intelligence database without knowing who might use such information and for what purpose (Ratcliffe & Walden 2010). In fact, these interactions are likely to constitute the majority of intelligence sharing.

Collaborative interaction

Collaborative interaction refers to intelligence sharing that is characterised by greater reciprocity among two or more agencies. Information may lead collaborating agencies to ask new questions that require additional intelligence gathering, thereby creating an iterative process of collection and analysis.

Type of connectivity

'Connectivity' refers to the way in which information is shared between entities. At its simplest, information sharing involves an exchange between just two entities (bilateral connectivity). This can be as simple as one law enforcement officer phoning another to obtain a particular piece of information.

Bilateral connectivity

In cases of bilateral connectivity, the provision of information is often narrowly defined between two entities. This may be based on a request for specific information, or it may be unsolicited information that is sent out to a receiving agency. Bilateral connectivity may also involve more person-to-person transfer of information than other forms of connectivity. This may particularly be the case where the goal of the information sharing is to share knowledge and experience between individuals (Jackson 2014). Liaison officers and multi-agency task forces both share information in a way that could typically be described as bilateral connectivity.

Liaison officers are outposted, or seconded from one law enforcement agency to another. On an international scale, they may be co-located with a diplomatic mission and are sometimes given diplomatic status. They act as representatives for the home law enforcement agency and are the conduit for information to flow between agencies. They operate by building networks of trusted bilateral relationships that are intended to be used when either the home or host agency requires information, dialogue or support from the other agency. As such, they can act as 'facilitator, broker, negotiator and trustor' (den Boer 2010: 58). In some cases (as with Interpol and Europol), liaison officers will be located in units with liaison officers from other countries. While this may create multiple opportunities for collaboration, those relationships remain bilateral, between the home law enforcement agency and the one with whom the liaison officer is collaborating. Liaison officers will also often avoid involvement in investigations, instead focusing on more strategic liaison activities (Bigo 2000).

On the information sharing matrix, liaison officers will often play a Connected-Bilateral role, but might also be more collaborative in some instances. The benefit of this approach is the relative simplicity of implementation, relying on individual officers rather than technological solutions. The disadvantage from an information sharing perspective is that connectivity is constrained by the personal relationships between liaison officers and their contacts. The 'bandwidth' for information sharing transactions will be narrow for even the best of liaison officers.

Task forces have been recognised as an effective means of sharing information with other law enforcement agencies (McGarrell & Schlegel 1993; Parliamentary Joint Committee on Law Enforcement 2013; Perras & Lemieux 2010; Rickards 2016). They typically involve officers from multiple law enforcement agencies seconded to a host agency to address a particular form of criminality. As seconded members, they are able to access the IT systems of their home agencies and can legally share information with other members of the task force, thereby enabling a more comprehensive understanding of criminality to be developed. This information sharing within a task force setting is often made possible through a formal memorandum of understanding between the agency hosting the task force and the agencies seconding officers.

Task forces differ from liaison officers in that the former are typically focused on operations and investigations and work together over a limited time, while the targeted criminality remains a concern. Such task forces will typically play a Collaborative-Bilateral role, although the nature of the sharing may also push them towards a more centralised role. As with liaison officers, task forces are easy to implement and rely on the deployment of officers. They also overcome some of the cultural barriers to information sharing, particularly those associated with competition, distrust and mutuality, as members of the task force will work towards a common goal. However, as with liaison officers, task forces typically share information among a small group of individuals, resulting in siloing—those outside of the task force working on similar issues may be unaware of the information gathered by the task force.

Centralised connectivity

Centralised connectivity describes an information sharing structure in which multiple agencies send information to a central storage facility where it can be combined and analysed. This analysis may be undertaken by any one of the agencies providing the information, as is the case with the ACIC's Australian Criminal Intelligence Database (ACID), which holds criminal intelligence from all jurisdictions in Australia (Parliamentary Joint Committee on Law Enforcement 2013). Alternatively, analysis may be undertaken solely by the central authority receiving the information, which subsequently disseminates the derived intelligence products. This is a model often used by US Fusion Centers, which draw information from multiple sources to produce intelligence with the aim of preventing terrorism (Chermak et al. 2013; Monahan & Palmer 2009). Data hubs of this kind, which allow for information to be provided but not used by those providing it, can best be described as a Connected-Centralised model (Figure 1). In contrast, databases such as the ACIC's ACID can be described as a Collaborative-Centralised model in that several agencies may provide information, the information is visible to all and agencies can work together.

A benefit of centralised connectivity is that, by joining together data from multiple sources, it may help to address the linkage blindness that can result from siloing. Centralised connectivity can be achieved through technological solutions that automate data capture and collation (Plecas et al. 2011). However, these automated processes can be burdensome if they share so much data that it cannot be analysed (Jackson 2014), although this can also be exaggerated and used as an excuse for not sharing (Markle Foundation 2003). Centralised systems can also be criticised as being 'black holes' that suck in data but return little intelligence to the agencies providing the original information.

Networked connectivity

A third form of connectivity involves networked arrangements in which each law enforcement agency in the network stores its own information but allows other agencies in the network to access its holdings, essentially creating a 'free market' in information exchange between law enforcement agencies (Anderson 1989). This approach could involve any agency in the network accessing data holdings of each of the other agencies to view information pertinent to its own operational requirements. This could be a passive form of interaction, as described by a Connected-Networked model, in which the agency uses information made available by others but produces its own intelligence products without the active involvement of others in the network. Alternatively, it could be a more active form of interaction, as described by a Collaborative-Networked model, in which access to devolved data may subsequently lead to further engagement from network partners. This is the model envisaged by the Markle Foundation (2002) in support of US national security in the wake of 9/11.

In practice, law enforcement information sharing relying on fully networked connectivity is rare, although the ACIC's planned National Criminal Intelligence System appears to be a hybrid between a centralised and networked system. The system would give all law enforcement jurisdictions a search capacity but would rely on data being sent by each jurisdiction to a secure cloud (Hendry 2017). The benefits of such systems are that they potentially provide real-time access to information across jurisdictions, thereby preventing siloing and the problems associated with multiple jurisdictions following the same lines of inquiry. However, such approaches are likely to be difficult to implement because of both the legislation and the technology required. From a cultural perspective, they may also require a rebalancing of control over information, away from the centre of the network and towards those working at the edge—often in operational roles (Alberts & Hayes 2003). The focus therefore shifts from how to collect and store information to how to use it.

Comparing connectivity

The key difference between the three types of connectivity is how the information is accessed by the user. In the case of bilateral arrangements, the information will be provided on request by the owner of the information—described as retail sharing by Sales (2010). In the case of centralised systems, the supplier of the data will typically deposit the data in advance for use by the end user. The information supplied may be a set of data agreed with the central agency (warehouse sharing), or information may be provided in the expectation that it will be of use to others, known as volunteer sharing (Sales 2010). For networked configurations, the user will extract the information directly from the other agencies' systems. While access controls exist at each level, these will typically be more significant in bilateral arrangements than in networked arrangements, although in each case decisions are made about what information to disclose.

In general, information sharing varies from the least sophisticated, in the bottom left segment of Figure 1 (the Connected-Bilateral model), through to the most sophisticated in the top right segment (Collaborative-Networked). It should be noted, however, that the choice of information sharing model is context dependent. For an immigration officer who needs further information on a traveller flagged as being of interest, a call to a contact in the country of origin (the Connected-Bilateral model) may be the most efficient method of obtaining information. In contrast, a Collaborative-Networked model may be more desirable when building multi-jurisdictional regional, national or international information sharing arrangements where large volumes of data are used to produce timely intelligence products. Therefore, the most appropriate level of sophistication will depend on the desired outcome of sharing the information.

Discussion and conclusions

Recognising the desired end-state for an information sharing arrangement will help to identify the legislative, technical and cultural barriers that need to be addressed to achieve success. These barriers will vary according to the types of interaction and connectivity involved. For example, in the case of an outposted liaison officer playing a Connected-Bilateral role, technical barriers are likely to be minimal, extending no further than the need for remote access to the home agency's systems. Depending on with whom the information is shared, legislative barriers may also be minimal if the sharing is covered by the organisation's existing legislation. In contrast, cultural barriers may be significant where the information sharing is first dependent on building a relationship of trust and reciprocity.

At the other end of the spectrum, agencies that aspire to Collaborative-Networked information sharing are likely to experience legislative, technical and cultural barriers. The ability to freely share information within the network may be restricted by the legislation governing each agency in the network. Different agencies may have different laws specifying how information can be disseminated and to whom, requiring legislative changes to be negotiated on a case-by-case basis. One advantage of this approach, however, is that the failure of one jurisdiction to change the necessary legislation does not preclude others in the network from sharing. Technical issues will focus on how nodes in the network can be connected, while cultural issues will focus on how to get law enforcement agencies to work together more interactively, once the information is made available.

Concluding remarks

This paper has demonstrated the benefits of law enforcement information sharing for criminal intelligence purposes, yet many hurdles to improving information flows remain. One small step towards addressing the legal, technical and cultural barriers to information sharing is to understand the nature of the information sharing mechanism, as defined by its level of interaction and connectivity. This helps to understand on the one hand the restrictions imposed by the information sharing context, and on the other hand the increasingly complex issues that are likely to be experienced as the level of sophistication grows.

References

URLs correct as at October 2018

Alberts DS & Hayes RE 2003. *Power to the edge: Command and control in the information age.* Command and Control Research Program Publication Series. US Department of Defense. http://www.dtic.mil/docs/citations/ADA457861

Anderson M 1989. *Policing the world: Interpol and the politics of international police co-operation.* Oxford: Clarendon Press

Aviram A & Tor A 2003. *Overcoming impediments to information sharing.* Harvard Law and Economics Discussion Paper no. 427. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=435600

Bichard M 2004. *The Bichard inquiry.* London: Stationery Office. http://dera.ioe.ac.uk/6394/1/report.pdf

Bigo D 2000. Liaison officers in Europe: New officers in the European security field, in Sheptycki JWE (ed), *Issues in transnational policing.* London: Routledge: 67–99

Carter D & Carter J 2009. The intelligence fusion process for state, local, and tribal law enforcement. *Criminal Justice and Behaviour* 36(12): 1323–1339

Chermak S, Carter J, Carter D, McGarrell E & Drew J 2013. Law enforcement's information sharing infrastructure: A national assessment. *Policy Quarterly* 16(2): 211–244

Commonwealth of Australia 2017. *Australian criminal intelligence management strategy 2017–20: Intelligence partnerships for a safer Australia.* https://www.afp.gov.au/about-us/publications-and-reports/australian-criminal-intelligence-model-acim-strategy

Connery D 2016. *For the right reasons, in the right ways (Part 1): A four-nation survey of information sharing about organised crime.* Canberra: Australian Strategic Policy Institute

den Boer M 2010. Towards a governance model of police cooperation in Europe: The twist between networks and bureaucracies, in Lemieux F (ed), *International police cooperation: Emerging issues, theory and practice.* Cullompton, Devon: Willan Publishing: 42–61

Guille L 2010. Police and judicial cooperation in Europe: bilateral versus multilateral cooperation, in Lemieux F (ed), *International police cooperation: Emerging issues, theory and practice.* Cullompton, Devon: Willan Publishing: 25–41

Hendry J 2017. National real-time intelligence sharing system edges closer. *IT News,* 13 Nov. https://www.itnews.com.au/news/national-real-time-intelligence-sharing-system-edges-closer-477101

Jackson AL & Brown M 2007. Ensuring efficiency, interagency cooperation, and protection of civil liberties: Shifting from a traditional model of policing to an intelligence-led policing (ILP) paradigm. *Criminal Justice Studies* 20(2): 111–129

Jackson BA 2014. *How do we know what information sharing is really worth? Exploring methodologies to measure the value of information sharing and fusion efforts.* RAND Corporation. https://www.rand.org/pubs/research_reports/RR380.readonline.html

Lemieux F 2010. Tackling transnational drug trafficking effectively: Assessing the outcomes of the Drug Enforcement Administration's international cooperation initiatives, in Lemieux F (ed), *International police cooperation: Emerging issues, theory and practice.* Cullompton, Devon: Willan Publishing: 260–280

Mapel M 2014. *Protecting those who protect us: Federal law enforcement deconfliction* (Master's thesis). Naval Postgraduate School, Monterey, California

Markle Foundation 2003. *Creating a trusted network for Homeland Security: Second report of the Markle Foundation Task Force.* https://www.markle.org/publications/666-creating-trusted-network-homeland-security

Markle Foundation 2002. *Protecting America's freedom in the information age: A report of the Markle Foundation Task Force.* https://www.markle.org/publications/667-protecting-americas-freedom-information-age

McGarrell E & Schlegel K 1993. The implementation of federally funded multijurisdictional drug task forces: Organizational structure and interagency relationships. *Journal of Criminal Justice* 21(3): 231–244

Monahan T & Palmer NA 2009. The emerging politics of DHS Fusion Centers. *Security Dialogue* 40(6): 617–636

National Commission on Terrorist Attacks Upon the United States 2004. *The 9/11 Commission Report: Final report of the National Commission on Terrorist Attacks upon the United States.* http://govinfo.library.unt.edu/911/report/

Occhipinti JD 2010. Parallel paths and productive partners: The EU and US on counter-terrorism, in Lemieux F (ed), *International police cooperation: Emerging issues, theory and practice.* Cullompton, Devon: Willan Publishing: 167–185

Parliamentary Joint Committee on Law Enforcement 2013. *Inquiry into the gathering and use of criminal intelligence.* Canberra: Australian Parliament

Perras C & Lemieux F 2010. Convergent models of police cooperation: The case of anti-organized crime and anti-terrorism in Canada, in Lemieux F (ed), **International police cooperation: Emerging issues, theory and practice.** Cullompton, Devon: Willan Publishing: 126–143

Plecas D, McCormick AV, Levine J, Neal P & Cohen IM 2011. Evidence-based solution to information sharing between law enforcement agencies. *Policing: An International Journal of Police Strategies & Management* 34(1): 120–134

Police Foundation 2016. *Best practices in event deconfliction.* https://www.calea.org/sites/default/files/EventDeconfliction_PoliceFoundation.pdf

Ratcliffe JH 2016. *Intelligence-led policing,* 2nd ed. Abingdon: Routledge

Ratcliffe JH & Walden K 2010. State police and the Intelligence Centre: A study of intelligence flow to and from the street. *International Association of Law Enforcement Intelligence Analysts Journal* 19(1): 1–19

Rickards C 2016. What are the barriers to gathering and sharing organised crime intelligence: An Australian perspective. *European Review of Organised Crime* 3(1): 78–104

Sales NA 2010. Share and share alike: Intelligence agencies, information sharing and national security. *George Washington Law Review* 78(2): 279–352

Schein EH 2017. *Organizational culture and leadership,* 5th ed. Hoboken, NJ: John Wiley and Sons

Sheptycki J 2017. The police intelligence division-of-labour. *Policing and Society* 27(6): 620–635

Sheptycki J 2004. Organisational pathologies in police intelligence systems: Some contributions to the lexicon of intelligence-led policing. *European Journal of Criminology* 1(3): 307–332

State Coroner of New South Wales 2017. *Inquest into the deaths arising from the Lindt Café siege: Findings and recommendations.* Glebe, NSW: Coroners Court of New South Wales. http://www.lindtinquest.justice.nsw.gov.au/

Taylor RW & Russell AL 2012. The failure of police 'fusion' centers and the concept of a national intelligence sharing plan. *Police Practice and Research* 13(2): 184–200

Whelan C 2016. Organisational culture and cultural change: A network perspective. *Australian and New Zealand Journal of Criminology* 49(4): 583–599

Dr Rick Brown is the Deputy Director of the Australian Institute of Criminology and Visiting Fellow of Policing and Criminal Justice at the University of Derby.

General editor, *Trends & issues in crime and criminal justice* series: Dr Rick Brown, Deputy Director, Australian Institute of Criminology. Note: *Trends & issues in crime and criminal justice* papers are peer reviewed. For a complete list and the full text of the papers in the *Trends & issues in crime and criminal justice* series, visit the AIC website at: aic.gov.au

ISSN 0817-8542

©Australian Institute of Criminology 2018

GPO Box 1936
Canberra ACT 2601, Australia
Tel: 02 6268 7166

Disclaimer: This research paper does not necessarily reflect the policy position of the Australian Government

aic.gov.au