SPECIAL REPORT

For the right reasons, in the right ways (Part 1)

A four-nation survey of information sharing about organised crime

David Connery

November 2016

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

STRATEGIC POLICING & LAW ENFORCEMENT PROGRAM

ASPI

David Connery

Dr David Connery joined ASPI as the Senior Analyst for the Strategic Policing and Law Enforcement Program in August 2013. He is now Head of ASPI-Education.

This is an abridged version of a report submitted to the Churchill Memorial Trust in June 2016. Also available, upon request to the author, are annexes describing the context for information sharing about organised crime in each of the four nations visited in field work for the report, and explanations of the information-sharing mechanisms discussed during the visits. A list of interviews by country can also be provided.

Acknowledgements

Special thanks go to the Churchill Trust; the Rotary Clubs of Griffith, NSW; and Peter Jennings, the Executive Director at ASPI.

This report is dedicated to the 80 people interviewed for this project, for they work tirelessly to fight organised crime in their respective countries. It's hard to imagine what the world would be like if good people like them, and their thousands of colleagues, weren't willing to do so.

About ASPI

ASPI's aim is to promote Australia's security by contributing fresh ideas to strategic decision-making, and by helping to inform public discussion of strategic and defence issues. ASPI was established, and is partially funded, by the Australian Government as an independent, non-partisan policy institute. It is incorporated as a company, and is governed by a Council with broad membership. ASPI's core values are collegiality, originality & innovation, quality & excellence and independence.

ASPI's publications—including this paper—are not intended in any way to express or reflect the views of the Australian Government. The opinions and recommendations in this paper are published by ASPI to promote public debate and understanding of strategic and defence issues. They reflect the personal views of the author(s) and should not be seen as representing the formal position of ASPI on any particular issue.

Important disclaimer

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional person.

Cover image: Graphic of information sharing on computer keyboard © Maksim Kabakou / Shutterstock

For the right reasons, in the right ways (Part 1)

A four-nation survey of information sharing about organised crime

David Connery

November 2016

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE
STRATEGIC POLICING & LAW ENFORCEMENT PROGRAM

© The Australian Strategic Policy Institute Limited 2016

This publication is subject to copyright. Except as permitted under the *Copyright Act 1968*, no part of it may in any form or by any means (electronic, mechanical, microcopying, photocopying, recording or otherwise) be reproduced, stored in a retrieval system or transmitted without prior written permission. Enquiries should be addressed to the publishers. Notwithstanding the above, Educational Institutions (including Schools, Independent Colleges, Universities, and TAFEs) are granted permission to make copies of copyrighted works strictly for educational purposes without explicit permission from ASPI and free of charge.

First published November 2016

Published in Australia by the Australian Strategic Policy Institute

ASPI
Level 2
40 Macquarie Street
Barton ACT 2600
Australia

Tel + 61 2 6270 5100
Fax + 61 2 6273 9566
enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au

 Facebook.com/ASPI.org

 @ASPI_org

CONTENTS

EXECUTIVE SUMMARY

This special report examines how government, business and the community in four nations share information about organised crime. Its key finding is that the Australian Government, businesses and community as a whole must be open to new kinds of information sharing partnerships.

The report begins by defining information sharing as 'the trusted exchange of relevant knowledge or data between organisations to achieve their mutual objectives'. The types of information shared are then divided into two: case information that involves data about individuals who are usually suspected of involvement in criminal activity; and bulk data that includes people in a given set regardless of any possible connection with crime.

The field work involved over 80 interviews, including visits to or discussions about a range of information sharing mechanisms in Israel, the UK, the Netherlands and the US. Those mechanisms were broadly differentiated by their location (within or outside government) and the nature of the sharing interaction (exchange or collaboration).

The variety of mechanisms used in the four selected nations shows that information sharing is valued and strongly shaped by the particular national context. This means some countries rely heavily on informal systems, others have large numbers of specialised exchanges, and some are more risk accepting in their arrangements than others. The field work showed that a wide range of options for sharing information about crime exist, and Australian authorities and businesses might wish to consider a number of them in more detail.

This research found both upsides and downsides to information sharing about crime. Some benefits are clear, including the opportunity to shape better interventions and build economy of effort in activities. While these upsides are undoubtedly attractive, it seems that the possible downsides of sharing—such as loss of control, the potential to compromise sensitive activities or an unwillingness to risk breaking laws, including those around privacy—were viewed as considerably strong downsides to sharing.

Still, it's clear that sharing must occur. That's because the scale of the challenge posed by organised crime—and the speed, reach and depth of penetration that the internet enables—means information sharing is critical for all three groups.

This report explains that information sharing is best promoted by building a strong sense of shared interest among the participants and then developing a strong system for information sharing that's governed by understood rules. This finding stands in contrast to those who emphasise interpersonal trust as the basis for sharing.

Factors that work against information sharing about crime include legislative barriers and complexity, poor value propositions around sharing, the self-conceptions of the actors and what they value information for, and cultural barriers. Such barriers include a culture of secrecy in government, a lack of willingness to expose possible flaws, and the view that 'information is power'. These are perhaps the most powerful inhibitors to sharing.

Efforts to enhance Australia's methods of sharing information about organised crime should be designed to cope with these inhibitors while making best use of the factors that promote this activity. Options for hosting information sharing organisations outside government, accepting a greater role for private funding for law enforcement activities, and encouragement of commercial efforts to gather and collate information, should all be considered by the Australian Government as it looks for new ways to undermine organised crime.

1. LOOKING FOR OPTIONS

'All that is necessary for the triumph of evil is for good men to do nothing.'

—The memorial tribute to Donald Mackay, 1933–1977

The problem

Information is an important commodity that, if released carelessly, can't be controlled. This property makes information sharing a very sensitive action because done in the wrong way, so that information falls into criminal hands or maligns lawful individuals, the act of sharing could have serious repercussions for justice, law enforcement and the community at large. That situation is in nobody's interest.

Information is the lifeblood of modern law enforcement, but the information needed by law enforcement isn't held in a single repository. Far from it. Information holdings are highly diffuse, and important evidence can be held not only by other government departments, but also by businesses and the public. Holdings can also be insecure, providing a tempting target for hackers and thieves. So bringing the right information together in the right way, form and time is an immense shared challenge for all concerned in this activity.

Finding suitable ways to share information about organised crime is therefore a critical task for Australia's governments, business sectors and community. This is particularly so as major debates rage about the balance between security and civil liberties; the retention and use of data and privacy; the valid role of encryption; and the increasing austerity being imposed on government and businesses directly and the public at large indirectly. Identifying ways to effectively and fairly share timely information and bulk data is a task that's becoming more challenging every day. New ideas are needed, and it's possible for Australia to find some different models for sharing by examining overseas experiences and practices.

Aim and method

This report examines three information-sharing relationships—among government agencies (especially law enforcement), the business sector and the community—in Israel, the UK, the Netherlands and the US.

The aim is to identify the basic frameworks used to share information about crime, especially but not only organised crime. This framework necessarily includes definitions of the subjects of the study (the actors involved) and the object (enhanced information sharing). The resulting framework is illustrated with examples from the four selected countries, which were visited during the field work phase. The study also identifies general factors that promote or inhibit information sharing about crime.

Field work for this report was made possible by a fellowship from the Winston Churchill Memorial Trust. More specifically, the fellowship is supported by the Rotary Clubs of Griffith, NSW, which maintain the Donald Mackay Fellowship for research into countering organised crime.

Research for this report was based on a review of the relevant literature and interviews with more than 80 experts from the government, community and business sectors of the four nations visited. Those countries were chosen

for the study because they are all liberal constitutional democracies, have significant safeguards in place to protect privacy, and conduct information sharing about crime. These criteria mean the types of mechanisms used (or not) are likely to be relevant to Australia. Semistructured interviews were used with each of the experts, nearly all lasted 90–120 minutes, and many were amplified in follow-up correspondence. The results of the study include assessments of the factors promoting or inhibiting information sharing in each country, a description of the mechanisms used and a model that allows information-sharing mechanisms to be categorised.

Report structure

The remainder of this report is structured into four substantive sections. The first defines the subjects of the study—organised crime and the government–business–community 'triangle' that needs to cooperate against these criminal actors. The second section describes the object of cooperation—information sharing—by defining it and then examining the reasons, types, risks and rationale for sharing. The third section develops a model for information sharing that's based on examples observed during the four-nation study tour. The final section draws conclusions for the study in the form of general factors that inhibit or promote information sharing about organised crime.

2. THE SUBJECTS

This research report is essentially about the relationships between and among two different subject groups. On one side sits organised crime: a broad grouping of nefarious actors who use criminal methods to exploit illicit and legitimate markets for private gain. The relationships among organised crime actors are not a topic for discussion here, but relationships among the second group are. This group is the government, the business sector and the community: a 'triangle' of actors who share—at least to some degree—an interest in combating organised crime. This section describes each actor group at its most general level as a way to frame the later discussion of information sharing.

Transnational, serious and organised crime

Defining transnational, serious and organised crime succinctly and comprehensively is difficult.

As my colleagues identified in a recent special report for ASPI, there are around 180 definitions of organised crime (as this activity and actor group will be called throughout).[1] Some require the presence of an ongoing criminal activity that uses methods such as money laundering, identity crime, violence, corruption and extortion to achieve the criminals' goals. Others are broader, focusing more on the seriousness of the crime or the criminals' capacity to operate across jurisdictions.

Organised crime operates in illicit markets, in legitimate markets and in any 'grey areas' that might exist—indeed, anywhere criminal attitudes and methods can be used to advantage in the pursuit of profit and self-preservation (although criminals can be interested in power, honour and gratification, too).

What's more, organised crime has evolved over the past few decades in ways that move beyond the hierarchical 'mafia' organisational styles that featured among the first definitions of organised crime. The old-style gangs have now been joined by more amorphous and fluid networks of actors who provide services or share tasks among themselves to their mutual criminal benefit.

In addition, the following characteristics usually apply to organised crime:

- It generally works in illicit markets but it exploits legitimate markets, too.
- There's an important financial dimension, particularly in efforts to launder money, hide criminal wealth through complex structures, attack victims' financial assets or intermingle legitimate trade and business with criminal activities. These crimes are often supported by 'professional facilitators' with legal, accounting or financial expertise.
- Violence was once considered a defining characteristic of organised crime. However, the cyber environment is now an important vector and target for organised criminal acts and major frauds that undermine economic strength, so violence might not always be present today.[2]

Serious and organised crime can be organised and perpetrated solely within one country ('domestic'), but it's very common for groups to have overseas, or 'transnational', links today. Transnational crime involves criminal groups that operate in more than one national jurisdiction, or crimes that are prepared in or have effects in more

than one country. As a result of this transnational trend, it's becoming increasingly difficult to identify the location of the source, all possible harms and the responsible jurisdiction for serious and organised crime. So, while the transnational element needs to be highlighted and is routinely serious, this report sticks with the term 'organised crime' for simplicity's sake.

The triangle of shared interests

The government, business and community sectors are considered in this paper as a triangle linked by their shared interest in combating organised crime. This is a heroic assumption. There are differences in attitudes, commitment and resources within these groups, so each contains subsets that warrant explanation. The groups also change over time, as some elements of each group evolve or play different roles at different times, as the media does.

The first actor group of the triangle is the government, of which law enforcement agencies are a key subset. These agencies are given, by law or accepted practice, a role in the criminal justice system that might include research, criminal intelligence, investigation, public safety, prosecution, judgement and correction. A range of other agencies with roles including policy setting, national security information protection, foreign affairs and regulation also play roles in the justice system. Of these peripheral justice actors, regulators are especially important because they may have the ability to set rules, conduct investigations and take briefs of evidence to the police or prosecution services. The government might also form subgroups that create links with the other actors. They might include public–private partnerships, taskforces that operate within public agencies, and international partners. Social service, economic and defence agencies are also likely to be relevant to fighting organised crime, even though their primary responsibilities lie in other areas.

The second actor group comprises businesses, which are profit-making entities that deliver goods or services in a market. Major business entities are usually incorporated by law, and many are regulated by government agencies. This group can be subdivided into those that provide services similar or complementary to law enforcement (such as physical security, cybersecurity firms and forensic analysis services) and the much larger grouping that relies on law enforcement and regulation to sustain suitable market conditions. Some overlap exists between these subgroups—security firms are also regulated and rely on a market, some large trading companies have investigative units that help law enforcement, and financial firms play a key role in the anti-money-laundering and counterterrorism financing (AML/CTF) system—so the distinction within this grouping isn't applied rigidly. Nor should the ability of business and law enforcement to 'cross over' be neglected. In the examples below, I discuss some in which business directly funds law enforcement agencies and some in which businesses are 'co-providers' of security.

The third group is the community, which comprises the individuals in society (the general public); academics and think tanks who conduct research and contest policy advice; and groups of individuals who come together to satisfy their mutual non-economic interests (often called 'not-for-profit', 'civil society' or 'third sector' groups). Not-for-profit (NFP) groups play different roles in society and, as we'll see, can be involved in two-way information sharing and partnerships with law enforcement under certain circumstances. NFP groups might also provide complementary services to government and business, such as welfare and social housing services. In all circumstances, NFPs, researchers and the general public are the recipients of police information (warnings and crime-prevention advice) and are sources of information about specific crimes (often called 'tip-offs'). Some bring matters to public and government attention and recommend or advocate for particular solutions to national problems.[3] When operating in this way, some community groups can act like the media, albeit on a different scale.

The place of the media in this triangle is ambiguous. Assuming it operates separately from the government (as it does in Western democracies), the media can be a business with peculiar needs. It, too, needs protection and advice on crime prevention, but it also needs content: publishable information about organised crime. The media is also a reflection of the community—it reports on issues that matter to the community, gathers and represents community views, and provides an outlet for members of the community to express views. This ambiguity means the media is well represented in the middle of the triangle of shared interests.

Linking these groups is clearly challenging, for another filter must be used: their desire, willingness and capacity to counter organised crime. We can't assume that every element in the triangle of shared interests shares the common goal described here. For instance, some professionals, such as some lawyers, accountants and real estate agents, facilitate organised crime by helping criminals to enter or operate through the legitimate economy. Some members of the public are supportive or tolerant of organised crime. Some members of government might be corrupted by crime. The role played by these elements is not considered further in this report, so we can focus on the key issue.

That key issue is straightforward: countering organised crime isn't the sole responsibility of any one group over another. Each has a part to play. Further, they can best perform their roles and achieve their individual and shared objectives if each hardens itself against organised crime by reducing vulnerabilities and by sharing information with the others.

That doesn't mean information sharing is easy or that its many complications have been overcome. Indeed, the 2015 version of Australia's National Organised Crime Response Plan highlights the weaknesses in information sharing between government, business and the community.[4] Before this report examines the different models for how information sharing is done in overseas jurisdictions, it's worth defining the topic and establishing its utility. After all, we shouldn't assume that sharing information about organised crime is unambiguously good.

3. THE OBJECT

Defining information sharing

Information sharing is the object of the relationships within the triangle of shared interests. While a seemingly straightforward concept, information sharing can be viewed in very different ways. A mechanistic view sees it as a function of taking inputs and creating outputs:

> Information sharing in criminal justice involves collecting and organising facts and figures (i.e. data), giving context to data, and providing information to various other individuals and/or organisations for strategic and operational decision making.[5]

> Information sharing involves the transfer of information from one agency to another.[6]

Others see information sharing as a social activity:

> Information sharing can be a volunteer behavior to provide information to other people who have information needs.[7]

Or they define it in a way suited to their specific sector. In an example pertaining to technology industries, the authors define information sharing as:

> … the exchange of a variety of network and information security related information such as risks, vulnerabilities, threats and internal security issues as well as good practice.[8]

Some use intelligence sharing as a synonym for information sharing, but we'll keep the terms separate. That's because intelligence is best understood as information collected, analysed and disseminated for a specific purpose and audience. That means the action of information sharing is only one part of the process of creating intelligence, even where intelligence product created by and for one organisation is given to another. In most cases, the receiving organisation must still analyse that product to determine its relevance, which creates a new product.

So in this report, information sharing is defined in socio-mechanical terms as the trusted exchange of relevant knowledge or data between organisations to achieve their mutual objectives.

While it's a start, that definition doesn't capture the distinctions between the types of information that can be shared, or different types of sharing mechanisms that can be used. These are important because the information-sharing activity will often be enabled or constrained by additional factors, such as law, needs and working culture.

Types of information shared

It's important to distinguish between the types of information about organised crime that can be shared, because one type tends to be less problematic in law than the other. Leaving aside the informal 'tips' that pass between individuals, formal systems often involve two broad types of information: 'case information' and 'bulk data'.

Case information is characterised by the direct exchange of data based on a specific request. The information provided often includes names, personal details, locations, details of assets, transaction records and the like. In most circumstances, case information is provided after a direct request is made about a particular individual and processed to one level or another. So shared case information might simply be individual pieces of data—or it might be fully-formed intelligence reports that, as noted above, the receiving organisation will still need to analyse that product for relevance. What's most important here is that the case information is directly relevant to a particular request, and limited by that request.

In contrast, 'bulk data' is structured or unstructured datasets concerning a relevant activity.[9] Bulk data might be used for research and intelligence purposes to examine the activities of many people at the same time, perhaps with the aim of isolating criminal activity and identifying an individual perpetrator. It includes references to more than one individual—often thousands at a time—and, unless it's 'scrubbed', will often contain personally identifiable information. As a result, bulk data tends to contain information about a number of people who aren't involved in crime, as well as about people who are.

Both types of information can be shared, but case information (when exchanged between authorised groups) tends to be less problematic. That's because it's usually highly specific, and standards such as 'suspicion' of involvement in a crime can be applied more readily to judge whether release is appropriate. This survey found numerous instances in all four national jurisdictions where such information is routinely, safely and expeditiously shared.

Bulk data can be shared, too, and it often is. For instance, de-identified crime statistics can often be provided to researchers and the public with little controversy. Publicly available bulk data (the extent of which varies from jurisdiction to jurisdiction) is also less of a concern. However, bulk data that can be used to identify individuals, especially those not suspected of crimes, tends to be highly concerning and broadly illegal in the jurisdictions surveyed for this report. Known for facilitating what are pejoratively called 'fishing expeditions', this type of data sharing can come afoul of informed consent and proportionality provisions in some legislation.

Types of sharing arrangements

The report also distinguishes between 'information transfer' and 'information collaboration' as types of information-sharing arrangements.

Societies are always engaged in the information transfer business: this involves the straight passage of useful information from one party to another. For example, the general public will nearly always provide 'tips' to the police, NFPs may examine crime areas and provide reports, and businesses will provide information as required by law, such as suspicious matter reports. For their part, police will provide warnings to the community and business about threats and give advice to prevent crime. There are very limited interactions between the sources, though, and when interaction occurs it tends to be in the form of sequential responses to each other.

Information collaboration is different. This activity usually occurs within formal, structured systems, where the partners work together to solve shared problems through the exchange of information. Sharing is interactive, trusted, based on agreed rules and often in real time. This report highlights a number of collaborations and identifies factors that allow these bodies to function within the law, achieve the defined purpose and operate sustainably in ways that satisfy partners, oversight mechanisms and the general public.

We shouldn't infer that one type of arrangement is superior to another from this categorisation. As with most things, it's more important to have the most appropriate arrangement to share than to have the one that sounds the most modern. This means that choosing the best form requires a keen understanding of why information sharing is needed in the first place, and the upside and downside risks associated with the options for sharing.

Potential benefits and downsides

The hypothesis under examination in this project holds that sharing information about organised crime has benefits for the national interest, economy and community as a whole. Cooperation between government, business and the community is needed to reap these benefits, which include the following:

- **Understanding the problem.** Shared information can help identify the scope and scale of a problem, relationships between actors involved in the problem, and the pattern of the actors' interactions in time and space. Since information sharing also increases the number of people engaged in problem solving and so introduces additional diversity into analysis, there's a chance to enhance assessments by integrating or testing different perspectives.[10]
- **Best use of the powers available.** Information sharing can promote cooperation among legitimate actors, including by promoting an understanding of the powers and capabilities of each. This can reduce overlap and increase the incentives to cooperate.
- **Better interventions.** Understanding the respective strengths, weaknesses, motives and methods of the actors involved (especially those causing threats to the community) helps legitimate actors identify ways to protect themselves, prevent access by illegitimate actors, respond to threats and recover from attacks. Information sharing promotes cooperation as shared objectives are established and a common awareness of the situation is developed. Information from government, business and community sources is also a key input to intelligence-led policing models.[11]
- **Economy of effort.** An adage in the information sharing business goes, 'Collect once, share many times'. Information sharing can (should) reduce the amount of effort expended to collect data, reduce the frequency of information requests from businesses and the public, and increase the utility of each individual dataset. Agencies can also be more specialised in their data collection and so reduce duplication of efforts and encourage compliance with law. In some ways, information sharing can make government less intrusive because fewer agencies need to collect the same data.[12]

Still, information sharing can have downsides. These negative consequences are often privileged in professional interactions that might warrant information sharing—leading to limited or no sharing between the parties at the extreme. The key downsides include the following:

- **Compromise of methods and sources.** Releasing information can sometimes reveal to others the method used to obtain the information, or the source of the information.
- **Compromise of operational activities.** The inappropriate release of information about operational activities, such as investigations, can lead to the compromise of evidence and make the activities unsafe for participants.
- **Breaches of rights, laws and freedoms.** The release of information has the potential to breach rights such as privacy or data protection laws in many countries. In other cases, sharing information about citizens raises the prospect of a 'surveillance state' in which information given by customers to business is used by government agencies to unnecessarily track law-abiding people. Some countries' authoritarian governments and the existence of laws incompatible with Western human rights standards complicate this risk when information gained domestically is shared with other countries.
- **Loss of context.** Data released can sometimes be stripped of its context. Aside from the mistakes non-experts might make in assessing specialised data, other problems with interpretation can occur once data has left the originating agency. For example, people might be admitted to a mental health program for a number of reasons and for conditions of varying severity. Therefore, assuming that a person has a serious mental health issue based on admissions data isn't necessarily justified.
- **Conferring unequal advantage.** Information sharing with selected partners can confer an advantage on one party that similar parties won't get. This might include insights into market conditions or competitor vulnerabilities. This risk is most relevant in small information-sharing forums where smaller companies or average citizens don't have the resources to participate.

- **Reducing relative advantage.** If information is power, releasing information can reduce the relative advantage of one party over another or complicate the working lives of those who must now answer more questions about their activities because 'outsiders' now know about those activities.
- **Imbalance between effort and reward.** Information sharing isn't a cost-free activity. New datasets may be required, data may need to be scrubbed of personally identifiable information or presented in different formats, people will need to assemble and reply to requests, and people may be asked to participate in taskforces or working groups. All of those activities cost money, and it may be that little is returned for that effort. Situations like this can lead managers to see information sharing as unwarranted and uneconomic for them.
- **Self-incrimination.** Sharing information might provide others with evidence of wrongdoing, poor practices or vulnerabilities.
- **Missed opportunities.** The decision not to share might mean that opportunities to address problems, create new value or save money are missed.
- **Unmet responsibilities.** The failure to share information can also result in severe criticisms of organisations, as the US intelligence community found after the 9/11 terrorist attacks, or in cases where real harm that befalls vulnerable people may have been avoided if agencies shared information.

While the downsides are more numerous that the identified benefits, that shouldn't discourage well-planned efforts to share information. Fortunately, a number of different models (described in Section 4) can be used to ensure that information sharing is healthy and cost-effective. Also, different kinds of information can be shared. This distinction is important because sharing some data to counter organised crime is usually considered legitimate, while sharing other types of data raises privacy and other concerns.

What information do government, business and the community want to share about organised crime?

The remarks above address the potential hazards of sharing information about organised crime. What needs to be addressed next is the type of information that can or should be shared. The needs and wants of each group can not only differ, but be in stark contrast with each other.

Government

In general terms, government needs can be divided into two levels. On a broad level, government wants to show action against visible crime, and this may include meeting election or policy commitments. Government also wants to advertise its achievements, be that through improved crime statistics or successful operations and initiatives. Satisfying this type of information need usually involves statistical data or reports on major police activities. Detailed evaluations might also help explain and advertise successful programs.

Law enforcement's main needs revolve around 'actionable' information. This might be information that adds to an intelligence picture, but information that helps investigations is most prized. This preference reflects the primary self-conception of most law enforcement agencies (especially police agencies) as being responsible for bringing criminals to account through the courts.

Law enforcement also needs information from business and the community about ways to fight crime. In particular, many large business have considerable experience in fighting crime in their industry sectors (including overseas sources of information), while others have specialist intelligence, forensic or technical skills. Sharing this kind of information can help law enforcement to warn, prosecute or protect, and commercial relationships may be established to provide this kind of information sharing.

Business

Businesses' desires for information differ in many respects, but they are linked around a tight focus on competitiveness and business survival. This means businesses want information tailored to their need for protection from crime, especially their immediate needs. They express a very uneven desire to receive broad, generalised information, but most appreciate and prefer tailored advice and threat alerts. There seems to be some interest—but not much—in forward-looking advice about emerging threats, new technologies and vulnerabilities, and ways to protect themselves from the attendant criminal threats.

Businesses also desire very specific information about criminal threats and methods, right down to the identity of customers who are criminal threats to them. This type of information might include account details, advice of fraudulent claims made against other businesses, or images of criminals.[13] Others, especially internet service providers and larger corporations, want details of cyber threats such as IP addresses and identities so they can take action to block malicious activity. This information represents their 'actionable intelligence'. However, it's possible that businesses want information that's further up the chain of discovery, but don't know how to ask. That information would be generated as new threats are identified, and involves businesses and law enforcement working collaboratively on 'joint discovery' of both criminal methodologies and perpetrators.[14] Such collaboration can already be seen in some of the information-sharing mechanisms described in the next section.

A third type of desired information is about particular events and emergencies that may affect business operations or continuity. This type of information also needs to be made as specific as possible, largely because information that's difficult to use can create confusion and increase costs.

What links these information desires is relevance and immediacy, and this is where government and business tend to diverge. Governments—especially at the federal or national level—generally want to deal with information on a large scale, involving the largest number of people possible. That doesn't preclude very direct and intimate sharing arrangements, as the examples in Section 4 show. But intimate sharing is costly for government and gets harder to achieve as the number of interested businesses increases. Scale is preferred, as it's cheaper to deliver.

Timely information can also be hard to share. Sharing with business might be contrary to the interests of law enforcement agencies, especially when legislation prohibits sharing or where investigations or court proceedings are underway. By the same token, businesses don't want to share information that might incriminate them or expose their wrongdoing. This reticence is particularly strong when disclosure to those who regulate them, or might hold them accountable to the law, might open the firm to penalties or even criminal prosecution. Disclosure might also expose the business to reputational damage, which for many presents a key risk and is an inhibitor to sharing.

That said, there are a number of ways that government and business are sharing information in intimate ways in all four nations visited, which gives room for optimism about the prospects for finding effective information-sharing mechanisms in different circumstances.

The community

It's harder to pinpoint what kind of information the community wants to receive and share. Certainly, accurate information to meet community members' needs is a longstanding desire. What seems to be changing is the desire for more specific information tailored to the individual's needs. This may involve alerts and warnings applicable to their 'microclimate' or neighbourhood. It might also involve specific crime prevention advice.

The information that the community's willing to share is highly contextual. As the Pew Research Center found through a recent survey:

> … the phrase that best captures Americans' views on the choice between privacy vs. disclosure of personal information is, 'It depends.' People's views on the key tradeoff of the modern, digital economy—namely, that

> consumers offer information about themselves in exchange for something of value—are shaped by both the conditions of the deal and the circumstances of their lives.[15]

But, willing or not, people are sharing more and more personal information and detailed information about their activities. While this isn't the place to explore the factors relating to individual information-sharing decisions, three drivers of that sharing are clear.

First, there's been a huge increase in the amount of information about individuals available to criminals, law enforcers and businesses. That increase introduces challenges for information storage, security and analysis. It increases the cost of holding data and encourages holders to monetise the data. There's also a greater chance for others to analyse the data for different purposes, such as criminal investigations. Inconsistent security standards among holders also increase the risk that data will be stolen and misused.

Second, actors have different interests in such information—although those interests can be symbiotic at times. For instance, many companies collect masses of data about their customers, and they might on-sell that to other business for marketing purposes. That same data, especially data relating to a person's identity or credit card, also provides a lucrative trove for criminal groups. Police investigations routinely use information from companies, especially telecommunications metadata, transport bookings and the like. The different ways data can be shared, used and repurposed mean that the consumer really has little say in who gets access after they provide it.

And third, businesses can help people, including criminals, by providing services such as encryption or anonymous account holdings that disguise data. These services complicate information sharing and frustrate law enforcers, tax departments and regulators.

In all these cases, the public's role as a consumer differs widely. NFPs and researcher groups have more specialised information needs than the general community, and they are likely to be well placed to use that information. In some cases observed, NFPs provide services to government (such as accommodation and welfare) that put their information holdings on a par with those of some national governments. Researchers have long demonstrated their value to law enforcement, especially as the data and analyses become more valued by agencies.[16] Individuals can also play important roles in various initiatives to counter organised crime, such as by reporting their observations through web-based platforms.

As noted above, the media plays a special role as both a business and as an expression of the community. In the main, the first information the media wants is the '5W/Hs' (who, what, where, when, why, how), plus the opportunity to publish the more salacious details or to use investigative techniques to create exclusive content. The media may also cooperate with police to inform the public or to promote senior officers' views. An extension of this role led to an interesting initiative identified in field work in the US, where Comcast, a media enterprise, runs the 'Everyblock' system. This system both promotes Comcast's goal of obtaining local news and provides people with information about their local area ('neighbourhood') in considerable detail.

On balance, it's worth sharing information about crime

The common factor that links the desires and concerns of all three parties is the value each attributes to information from the others. While this assertion isn't backed by any survey, no person interviewed for this project has said that information shouldn't be shared, or that they didn't want better, clearer and timelier information. All recognised the importance of sharing in the right way, and many were open to new kinds of sharing relationships. All recognised the importance of some level of reciprocity, although that level differed in both volume and time.

To meet this desire, all parties need appropriate ways to share information in ways that serve their interests and meet their respective obligations. A number of different mechanisms, which sometimes follow very different approaches to meet these needs, were observed or discussed during the field work for this project. Some are described in the next section to illustrate the available range of mechanisms.

4. THE MECHANISMS

The dimensions of sharing

The field work conducted for this study identified two principal dimensions for describing formal information-sharing systems: location and working approach.

The mechanism's location—the degree to which it's inside or outside government—is important because it determines sources of funding, authorities for sharing and, ultimately, work priorities. It also influences the rules under which the mechanism operates and the information resources that it might draw upon. Those could include classified intelligence sources, open source information or information that others are compelled to supply by law.

The working approach taken within the mechanism falls along a continuum between information exchange and collaboration. No system observed for this study truly consists of one-way traffic. In real life, police provide information through one route but also receive information through the same or a similar one.

The important distinction between the two poles of this continuum is that information exchange doesn't involve an ability to develop new knowledge in a dynamic way, as collaboration does. In a typical exchange, the government takes information in and, sometime in the future, provides information out. The information 'in' might include suspicious matter reports from banks, closed circuit television images from building cameras, or reports of unusual purchases of sensitive items. Feedback will come, perhaps directly in alerts or indirectly in case studies or typologies.

In collaborative mechanisms, actors with shared interests work together and iteratively to solve problems. Resources are shared, information accumulates, working environments are generally close, and mutual benefits are accrued.[17] The working relationship is usually very close, often but not always involving co-location. Indeed, the ability to bridge distances through web-based technology has significant potential, and this might both improve the ability to collaborate and reduce costs for participation in the future.

Before examining how these dimensions interact, it's worth examining situations that lie outside this formal model.

Informal mechanisms

Of all the mechanisms, informal information sharing is the longest standing and most widely used. It's highly reliant upon personal networks, people who recognise the information needs of others, and trusted ways to share information. Trust is essential because sharers bear significant risk: there's the real potential for gain as new insights are produced and new options to solve problems come to light, but there are also potential downsides. In addition to those already mentioned, sharers without explicit authorisation to share could face sanctions if their conduct is called into question. Sharers also bear risk as to the quality of information, which might not be verifiable before it's employed. Informal systems can also disappear when people change jobs, and can suffer from degraded effectiveness until new relationships are built.

While informal information sharing may arise spontaneously and without official sanction, it's likely to be based on an existing formal arrangement. In these cases, the informal dimension of the sharing arrangement still has significant utility: it can increase the responsiveness of the formal system, create work-arounds when the formal system doesn't work, and increase the richness of information gained formally.[18]

It's interesting how most of the literature reviewed for this report refers only to information sharing among government agencies. There's little research that analyses how informal information sharing might work among government, business and the community when it comes to crime; indeed, information sharing of this type may be considered highly illegitimate.

Even where inter-sectoral information sharing about crime and security is described as 'informal', it still occurs within formally organised systems. For example, sharing information about critical infrastructure threats may occur 'informally' within systems like Australia's Trusted Information Sharing Network, but that network sanctioned the initial relationships among the sharers.[19]

That's perhaps why formal sharing mechanisms were those most often encountered in this research.

Formal mechanisms

Formal mechanisms involve written agreements between the parties to share information. The agreement is drafted to not only comply with relevant laws, but also to create shared expectations of each of the participants. In some cases, the agreement might be used to ensure recourse in case of some form of contravention, but punitive action is unlikely to be the key motivator for making the agreement. Rather, the key motivator lies in creating a trusted environment for collaboration so that individuals without personal relationships with each other can work together.

The field work for this project examined 27 different formal mechanisms for sharing information about crime in general. Using the two characteristics of location and working approach identified above, four basic kinds of formal mechanism can be discerned and illustrated through examples, which are described below (Figures 1 and 2).

Figure 1: A typology of formal mechanisms (location and type) for information sharing

Inside government – exchange

- Government agency takes information in
- Others may have reporting obligations
- Often uses web/email technology
- Generalised advice provided – later
- May involve 'networking' groups
- Focus on government interests

Outside government – exchange

- Civil organisation takes information in, often from members
- Created to provide advice or products to community or law enforcement (as intelligence packages / draft evidence briefs)
- Focus on industry interests

Inside government – collaborative

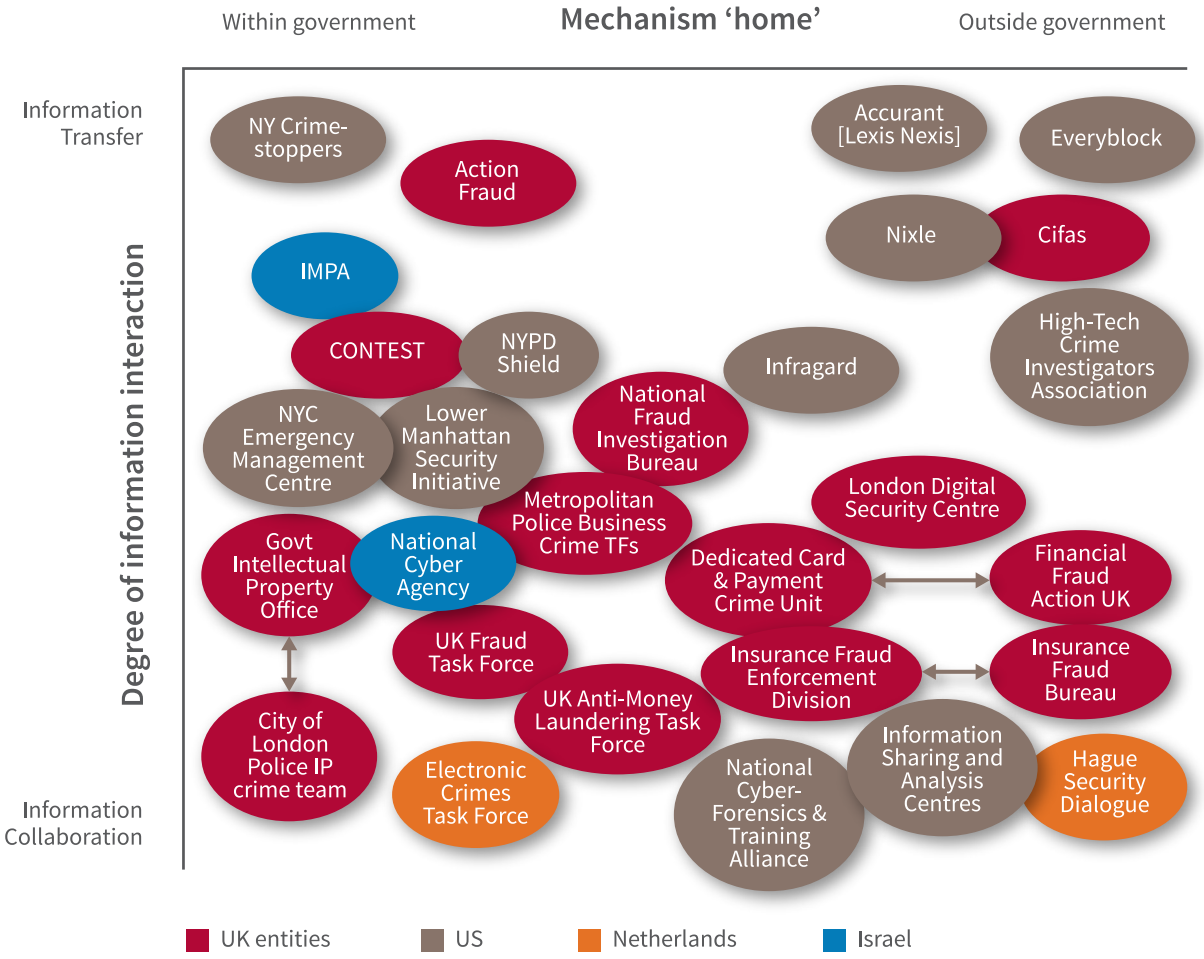
- Typically involves business or community representatives working inside government agency
- Real-time sharing on agreed priorities
- External organisations take and use information as they need it
- Case development before handoff for police–prosecutor action

Outside government – collaborative

- Often brings information from business to trade associations
- In UK, can be linked to sponsored police unit
- May involve technology and concept development

PPP = Public–Private Partnership

Figure 2: Information sharing mechanisms interaction/home matrix



Note: Positioning is approximate due to the large number of organisations that overlap in given areas of the matrix.

Red = UK entities; brown = US; orange = Netherlands; blue = Israel

Note: Positioning is approximate due to the large number of organisations that overlap in given areas of the matrix.

Inside government—information exchange: New York Crime Stoppers (US)

The Crime Stoppers program is run by a cell within the New York Police Department (NYPD). Its basic purpose is to provide a way for members of the community to provide information anonymously, and provide cash rewards where the information is used to make arrests. While the unit is part of the NYPD Detective Bureau, the reward money is provided by the NYPD Foundation. This creates an arm's length relationship between the taxpayer and those who receive the rewards.

Outside government—information exchange: Everyblock (US)

Everyblock (www.everyblock.com) is a web-based information service that operates in a number of major US cities. This service is provided by media corporation Comcast, and started as a way for local media organisations to remain abreast of events. It was also used as a way of providing local content to users at a time when news outlets were being amalgamated into larger units.

In today's format, Everyblock has also become a platform for police 'Open 311' information (non-emergency requests for assistance), council notices such as those about road closures and building permits, and events such as neighbourhood meetings and block parties.

Everyblock is managed as a business unit of Comcast. Most control is maintained locally by Comcast local media outlets, which maintain a moderating function on the bulletin board. The company is able to monitor direct take-up and use very accurately, and can also identify where its content is used by others.

Inside government—collaborative: Electronic Crimes Task Force (Netherlands)

Formed in March 2011, the Electronic Crimes Task Force (ECTF) is a partnership between the Dutch National Police, the National Public Prosecutor's Office and a number of financial institutions.[20] This unit is hosted within the National High Tech Crime Unit, a part of the Central Criminal Investigations Division, but its work is guided by a supervisory committee.

The committee is chaired by a deputy police commissioner and includes the National Cyber-Crimes Prosecutor, the Head of the High-Tech Crime Unit, representatives of all members (usually the heads of anti-fraud and compliance units) and a representative from the Ministry of Security and Justice. The committee meets every eight weeks. It doesn't provide operational direction to the taskforce, as that remains a police responsibility.

The ECTF has a complement of around 13 people, drawn from the National Police, business and other government partners. All ECTF partners sign a covenant, which sets out the role, legal basis, expectations and responsibilities of each member. Participants also agree to bear all costs associated with their participation, and assign at least one person to the ECTF. The office is a small room with 10 workstations.

The information shared within the ECTF is case information, in the form of responses to enquiries about a particular customer, transaction or account. The information is shared only within the boundaries of the ECTF.

This system requires a high level of trust in both the operational model and the individual involved. The taskforce is able to short-cut the usual processes, which can take months, and to respond to emerging threats and methods. Indeed, the ECTF prides itself on looking for the new methods, as it feels best placed to identify and analyse them.

Outside government—collaborative: National Cyber-Forensics and Training Alliance (US)

The National Cyber-Forensics and Training Alliance (NCFTA) is a US public–private partnership specialising in countering cyber threats through information sharing among and across industry and government within a trusted environment. Founded in 2002, it's focused on identifying, mitigating and neutralising cyber threats globally through three main programs: the Cyber Financial Program, the Brand & Consumer Protection Program and the Malware & Cyber Threats Program. The NCFTA is located within the FBI's Internet Crime Complaint Centre (IC3) in West Virginia.

The NCFTA was established as a 501(c)(3) non-profit corporation with a board of directors drawn from various sectors. It operates with a complement of around 100 people, about half of whom work for the NCFTA; the rest come from US and foreign law enforcement agencies and various industries. The NCFTA also has an extensive network of affiliates and member organisations in the US and overseas, and is closely associated with the FBI's Cyber Initiative and Resource Fusion Unit.[21] Its resource base isn't publicly disclosed.

The NCFTA operates by conducting real-time information sharing and analysis with subject matter experts in the public, private and academic sectors. Participants must sign a confidential membership agreement, and the alliance has strict non-disclosure requirements.

The type of information shared is case-based. The NCFTA uses communications platforms such as listservs, working groups and peer calls to discuss which issues are being seen in various industries and how best to address them. It also uses its Internet Fraud Alert system to report stolen account credentials discovered online.

The NCFTA enables close contact between private sector cyber and intelligence experts and experienced law enforcement officers to promote responsiveness, security and collaborative approaches to problem solving.

A model worth noting: Financial Fraud Action UK and the DCPCU (UK)

One last model worth noting belongs to the 'outside government—collaborative' sector, but it also straddles the 'inside government' sector due to some unique policing arrangements.

Financial Fraud Action UK (FFA UK) is responsible for leading the fight against fraud on behalf of the UK payments industry. Its membership includes banks, card issuers and card payment acquirers in the UK. Its focus is on non-competitive fraud issues. This sees FFA UK involved in an industry strategic threat management process, managing industry intelligence-sharing about fraud (the Financial Fraud Bureau), expert security assessments and outreach, including public affairs and awareness. FFA UK has close information-sharing relationships with the National Crime Agency, the National Fraud Intelligence Bureau and the Dedicated Card and Payment Crime Unit (DCPCU).

The DCPCU is a collaborative arrangement between the Metropolitan Police Service, the City of London Police and FFA UK. Importantly, it isn't part of a police force, but a collaborative arrangement between the three partner groups. It's managed by a board and receives administrative support from the City of London Police. It's operationally independent of all other organisations and agencies.

The DCPCU has around 39 people, and FFA UK has around 29 people. Both are fully sponsored by the banking industry: the DCPCU's annual funding of around £4 million is managed through FFA UK. The DCPCU is accommodated with FFA UK in adjacent offices.

Case information is the basis of sharing in this arrangement. Intelligence briefs or information about individuals or accounts is provided by banks or FFA UK to the DCPCU. The DCPCU has fraud investigators and liaison officers from industry as well. It also receives police information from other agencies.

This mechanism provides for very close relationships between industry and government. However, it was described as uncontroversial because its structure and practices allow the police unit to be at arm's length from individual companies and operationally independent. It's also clear that the arrangement adds additional resources to policing, as well as providing a home for specialised investigators.

A world of options—and opportunity

These mechanisms are only a sample of those studied during the field work for this project. Further examples can be found in the country studies, which can be obtained from the author upon request.

This survey highlights the wide variety of options available for information sharing, and the way business is willing to play a central role in them. The survey also shows that establishing a new information sharing mechanism might need government leadership at first, but continued leadership into maturity is not essential by any means.

Rather, the examples studied during the field work show that governments have many options to choose from, and that firms who are hit hard by crime are willing to collaborate very closely in order to reduce their losses. In some cases, this has included the direct financing of police-led investigative units. Such units expose a force to risk, but when managed well from the outset they can add resources to law enforcement without being a drag on already-stressed budgets. In other cases, it has led to very close information sharing partnerships that enable very intimate relationships in the common good.

New technology is also creating opportunities. Collating and analysing significant amounts of government-, business- and community-provided information is now very feasible. Additional commercial and public-interest uses can be found for that data. Safeguards can also be designed to ensure relevant laws are satisfied and community expectations can be met. Still, making this all work still requires close attention to the cultural, organisational, legal and technological factors that enable and inhibit information sharing about crime. These factors are explored in the final substantive section.

5. FACTORS AFFECTING INTER-SECTORAL SHARING

The field work for this report found that the four nations visited had different but broadly similar abilities to share information, albeit with authorities that varied even between like agencies. All had access to similar technologies for sharing. However, their practices and mechanisms were quite different.

This section draws conclusions for information sharing about crime in general, with a focus on the factors that enable and constrain inter-sectoral sharing. The conclusions are based on discussions with experts involved in the field and are tempered by the findings of literature examined for this project.

Enabling factors

Researchers have identified many factors that promote information sharing among different sectors.

Robinson and Disley identify economic incentives stemming from cost savings and incentives stemming from the quality, value and use of shared information as the two primary enablers.[22]

Yang and Maxwell examine three interrelated contexts for information sharing: interpersonal, intra-organisational and inter-organisational. At the interpersonal level, socialisation is both an influential factor and a process that facilitates information sharing, especially the sharing of explicit knowledge and tacit knowledge, between individuals. However, information-sharing behaviours become more complicated when individuals operate at the intra-organisational and inter-organisational levels. Understanding the enabling factors at these levels requires an analysis of culture, incentive systems, information technology, belief systems and political and legislative support.[23]

LeBuef and Pare emphasise personalised factors such as direct human contact, trust in people and processes, and support as their main promoting factors.[24]

Research for this report tends to support the broad findings of these scholars, but offers a slightly different emphasis and a completely different primary reason for sharing.

Indeed, research for this study found a shared sense of need as the primary reason why the three groups share information about crime. This is especially so in situations where businesses see a chance to reduce their losses and other risks by cooperating with government agencies. Government agencies also acknowledge their shortcomings and see value in cooperation with business, and are prepared to create suitable trusted mechanisms.

It's also important for government agencies to see the community as a potential collaborator in solving crime, and not only as a partner for information exchange. Admittedly, most of the current collaborative activity revolves around neighbourhood crime, which isn't necessarily about organised crime. Despite that, it's possible to see how web-based technologies could enhance government–public collaboration, especially for reporting the signs of organised crime, such as sales of counterfeit or illicit goods. Web technologies also have potential to deal with the challenges for government posed by the scale of information and provide necessary contact points for public involvement.

Shared needs, threats and goodwill are necessary for information sharing, but insufficient. In addition, information sharing must be positively enabled through political support, resources and legislation. Without such support, government agencies may lack the legitimacy to share and the ability to assign people and processes to create and maintain an effective and legal system. The needs of both business and the community must also be factored in, as those groups can help generate support, and they must see value in cooperation. That's especially so when participation in information sharing costs money, so businesses in particular must gain value worth the cost.

Mechanisms allowing businesses to share incriminating or potentially damaging information must also be devised to enable sharing. They might include immunities, delayed prosecutions, voluntary restitution or self-corrective action. Safeguards would also be needed, and may include protections from secondary uses of the information, for example in tax proceedings. Regardless of the forms of the mechanisms, devising them will be a difficult balancing act for all concerned, but at least having ways to encourage such disclosures will create conditions for voluntary information sharing about the most sensitive matters.

Of course, information sharing isn't always voluntary. Obligations, such as those imposed under AML/CTF regimes, also make sure information is passed from business to government. The result isn't always economical, for useful reports are said to be a small proportion of the total. Improving the ability to mine information provided in bulk should therefore be a priority for government agencies, so they can get more from what they hold.[25] Without additional attention and use, obligatory reporting appears costly and contains risk. That risk can materialise when unexploited data holdings are found to contain important pieces of information that might have prevented a crime.[26] The often slow feedback involved in this type of relationship tends to detract from the value of participation by businesses, in particular.

Smart structures also promote information sharing, and a number of them were studied during field work. When enabled by legislation, structures (and their enabling agreements) provide the forum and details of participation that legislation won't provide. But even lacking legislation, agencies and businesses can enter meaningful partnerships based on existing authorities or even general measures that help to fight crime.

The Dutch ECTF is a good example of such an arrangement. Creating arm's-length relationships between business and law enforcement has also helped to create high degrees of collaborative information sharing in both the US and the UK in fields including cybercrime and fraud. In the UK, the sponsorship of police units by business associations has added particular value: additional resources are created for law enforcement agencies, highly trained investigators are retained in units with a single focus, and the particular needs of an industry can be met expeditiously. While private sponsorship of policing is highly controversial in other contexts, the UK's approach doesn't appear to attract any controversy.

Structures also help to create trust. As mentioned above, there's some thought that interpersonal relationships are needed to establish the level of trust necessary to create effective sharing mechanisms. In many of the cases observed, the mechanism came before the relationship, and so information was shared before the trust was developed. In this way, good structures—based on agreed and known rules, secure communication and, ultimately, value—can create the conditions that allow information sharing to prosper.

On the other hand, it seems that when organisations become too large the ability to exchange sensitive information can go into decline. In a few of the mechanisms observed, large groups of unvetted people don't create good conditions for sharing. That doesn't make such groupings useless or dangerous—it just limits their utility. On the upside, people will meet through these arrangements, create relationships and find new ways to share the information they need. Web-based technology, which requires members to be accepted, can also promote good information sharing among large groups, but the information shared in such broad-based forums is likely to be low in sensitivity, untimely and potentially broadly focused.

At the opposite end, where informality rules, low levels of public scrutiny and oversight can also promote information sharing. The lack of security can effectively create space for information to be shared or traded, which raises concerns about legality, fairness and security. In today's climate, where such arrangements are often considered illegitimate, active steps might be taken to inhibit such information sharing.

Inhibiting factors

Of the main factors inhibiting information sharing, legislation is often cited first, for two reasons. First, privacy laws and the desire to avoid 'criminalising' legitimate daily activity can combine at different times to inhibit sharing. This is a concern about 'Big Brother', but the challenge is also reflected in the sheer volume of possible data that business and government agencies have and the public can provide. Anti-trust laws were also cited as a legal inhibitor in some countries. In these situations, companies might not be allowed to share information directly and need a third party such as a professional association or law enforcement facilitator, or enabling legislation such as the US PATRIOT Act, to manage that difficulty.[27]

Legislative complexity is the second reason. In some countries, it can be very hard to identify all of the legislation that affects information sharing, even when a guide is produced to provide a one-stop reference for sharing. That's because training is an additional piece of the puzzle, and it might not be provided before a person is brought into an information-sharing mechanism. Still, this inhibitor is solvable, and local facilitation measures can help.

Poor-quality information, whether it be too hard to digest or not valuable enough to justify the costs of sharing, was another inhibitor. In some of the larger mechanisms with thousands of members, the information passed is often no better than media reports. In other systems, unrefined information might simply swamp those with a small capacity to deal with it.

The lack of a two-way street for information sharing might be an inhibitor. This occurs especially in information exchange situations: there tends to be a long delay between information moving to government from business or the community and the government's return response to that information. This situation was especially noticeable in the banking sector, where formal requirements to share information led to an excess of information being provided to government, and frustration at the time taken for government to provide updated information about criminal trends and methods back to the banks. According to some interlocutors, this discourages active assistance and discrimination by businesses because the return is neither timely nor specific enough to warrant an investment in improving the quality of their sharing. Others point to the need to use the data better so that those providing information see more value for their contribution.

The cost versus return factor plays out in other ways. Some businesses may be reluctant to participate in sharing mechanisms that don't provide immediate returns for them. Others may lack the scale and resources to participate, especially where meetings and committees are required. This means that small and medium-sized companies (not to mention the general public) can be excluded from participating in information sharing. Yet when efforts are made to include those with more limited resources, a paradox arises because the mechanism is less trusted and the information is less tailored and less 'special'. Cost also figures in government calculations, too.

In some countries, distinctions between 'criminal' and 'national security' intelligence remain or have only recently been removed. This creates challenges for sharing these two related types of information because the systems in place don't necessarily allow easy movement between the two domains. This is particularly so because security clearances for people and information systems take time and money to change. In the US, formal procedures are needed to share information between these domains, and some believe that such sharing can't take place in any case.[28]

There also remains some tension between the standard 'need to know' principle for information sharing and the emerging norm of a 'duty to share'. This tension becomes evident when it remains up to the individual to know who needs the information at hand and means that established relationships are really the only ones serviced.[29]

The self-conception of law enforcement agencies, which places primacy on arrests and prosecution, can inhibit information sharing. In this frame, sharing information can impede their ability to prosecute because a 'premature' act could result in a mistrial or miscarriage of justice. It's this concern that often leads government agencies to hold on to valuable information until court proceedings are complete. This inhibition means that other criminals using the same methodology may continue to exploit a vulnerability for some time after the initial discovery.

Of all of the factors, most of those interviewed for this project agreed that 'culture' was the main inhibitor. What 'culture' meant was more difficult to unpack. For some, the 'culture of secrecy' was the key concern because it prevented relationships from forming in the first place. Many in government and business subscribe to this culture for a good reason, as information about crime is highly sensitive and can do harm to society if released in uncontrolled ways. While that's true, this reason doesn't account for every situation where sharing would be possible but doesn't occur, such as in cases relating to countering money laundering or fraud methodologies. For others, a culture of 'information is power' was dominant, even if this was harder to pinpoint with the research method used.

Yet culture can also be seen as an excuse. In a number of instances, a lack of understanding, complicated rules, costs and an absence of leadership can also explain the absence of sharing. That means the search for reasons why information isn't shared—and options for how this act can be improved—needs to take the widest possible scope.

6. CONCLUSION: FIND NEW WAYS TO SHARE

This four-nation survey of information sharing about organised crime, which was conducted with the support of the 2015–16 Donald Mackay Churchill Fellowship, was an opportunity to examine a number of different structures, processes and cultures of relevance to Australia. The systems studied varied greatly: they included the formal and informal; the impersonal and the intimate; and the technology-enabled and the 'old school'. All were different, some were undergoing review and change, and all had their place in their particular context.

The range of interviews undertaken covered all three actor groups in the 'triangle of shared interest'. While the interviews showed different perspectives on information sharing, they also showed strong support for the concept and offered different approaches to sharing.

This research found both upsides and downsides to sharing information about crime. There were many risks for those sharing, and those were often considered first and privileged in decisions. Still, it's clear that sharing must occur. That's because the scale of the challenge posed by organised crime—and the speed, reach and depth of penetration that the internet enables—makes information sharing critical for all three groups.

Finding optimal ways to achieve sharing is therefore a critical task, but it was clear from this research that no single way is 'the best'. Legislative factors, resources, threat and national style all played a role in identifying the preferred mode. What allowed that mode to be analysed were the common features of these information-sharing systems: the information shared (case-based or bulk data), the approach taken (exchange or collaboration) and the location (inside government or inside business). These attributes can be effectively combined to scope the field and identify different candidates for new system designs.

Yet, while the mechanisms differed, the major inhibitors and enablers of information sharing in these systems were relatively consistent across the national jurisdictions. This research found that shared need was perhaps the greatest enabler of information sharing, which means that building a sense of common purpose will be a vital step in the design and implementation of any system.

Next, creating a trusted system, which in turn enables legitimate information sharing, seemed to precede and transcend interpersonal trust, which is a factor others have seen as critical to sharing. At the risk of channelling old movies, 'build it (sensibly) and they will come' might be the best guide for designers of information-sharing systems.

That means openness to new kinds of partnerships is critical. Government led, funded and controlled is not the only model available. Indeed, the examples surveyed in this report shows that closed models are comparatively rare today. They've been replaced in many cases by models that bring the public sector and private sector into close partnerships, and use tailored governance arrangements to satisfy probity, financial and outcome purposes.

While legislation was often considered the greatest inhibitor, most participants described a reasonably enabling environment for sharing. Instead, much of the friction could be explained by culture. But this concept needs to be unpacked: are we talking about leadership, ways of working or education? Again, attention to all three is important and no one intervention is likely to overcome the inhibitions faced by those entrusted with sensitive information.

The next question for this research is, 'So, what for Australia'? The potential ways to answer that will be canvassed in Part 2 of this project. That work will aim to identify new approaches to thinking about information sharing, suggest legislative reforms, describe some possible structures, and identify education needs to bring the triangle of shared interests together in Australia so that they can share information about organised crime for the right reasons, and in the right ways.

NOTES AND ACRONYMS

1 D Connery, C Murphy, H Channer, *Web of harms: serious and organised crime and its impact on Australia's interests*, special report 81, ASPI, Canberra, 2015. The following section borrows heavily from pp. 3–4.

2 Australian Crime Commission (ACC), *Organised crime in Australia 2015*, ACC, Canberra.

3 For instance, the role of Israeli NFP groups in analysing and highlighting human trafficking in that country was mentioned in an interview as an example.

4 Attorney-General's Department, *National Organised Crime Response Plan 2015–18*, pp. 19–20, describes the community as 'underutilised' and notes that it's harder to gain traction to combat organised crime in industries whose profits are only marginally affected by it. There's also a general desire to reduce the cost of maintaining relevant government–business relationships. There's also a strong focus on enhancing information sharing within and between governments: while related, this challenge lies outside the scope of this paper.

5 D Plecas, A McCormaick, J Levine, P Neal, I Coen, 'Evidence-based solution to information sharing between law enforcement agencies', *Policing: An International Journal of Police Strategies and Management*, 2011, 34(1):121. See also Department of Homeland Security, *Local anti-terrorism information and intelligence sharing: overview*, n.d., p. 1, online.

6 UK Home Office, *National support framework: information sharing for community safety*, HM Government, 2010, p.5.

7 TM Yang, TA Maxwell, 'Information sharing in public organisations: a literature review of interpersonal, intra-organisational and inter-organisational success factors', Government Information Quarterly, 2011, 28:165.

8 Neil Robinson, Emma Disley, Incentives and challenges for information sharing in the context of network and information security, European Network and Information Security Agency, 2010, p. 9.

9 In general terms, 'structured' data has a high degree of organisation and may be contained in databases that are searchable by simple, straightforward search operations. Unstructured data is essentially the opposite and includes formats such as video and images (see Bright Planet, *Structured vs Unstructured data*, 28 June 2012, online).

10 Nathan A Sales, 'Mending walls: information sharing after the PATRIOT Act', *Texas Law Review*, 2009–10, 88:1801–1802.

11 JG Carter, 'Inter-organizational relationships and law enforcement information sharing post 11 September 2001', *Journal of Crime and Justice*, 2015, 38(4):523–524.

12 Sales 'Mending walls: information sharing after the PATRIOT Act', pp. 1798–1799.

13 Carter, 'Inter-organizational relationships and law enforcement information sharing post 11 September 2001', p.525.

14 Discussion with Australian Government official, 23 May 2016.

15 Lee Raine, Maeve Duggan, *Privacy and information sharing*, Pew Research Center, 14 January 2016.

16 For a discussion of this topic, see Malcolm K Sparrow, *Handcuffed: what holds policing back, and the keys to reform*, Brookings, Washington, 2016, especially chapters 3 and 4.

17 J-P Hatala, JG Lutta, 'Managing information sharing within an organizational setting: a social network perspective', *Performance Improvement Quarterly*, 2009, 21(4):5.

18 C Whelan, 'Informal social networks within and between organisations', *Policing: An International Journal of Police Strategies and Management*, 39(1):150-2.

19 See Australian Government, *Critical Infrastructure Resilience Strategy: plan*, Commonwealth of Australia, c. 2010, p. 3.

20 The full non-government membership list is ABN-AMRO, Rabobank, ING, SNS Bank, the Dutch Bankers Association and the International Cards Association.

21 Federal Bureau of Investigation, *The NCFTA: combining forces to fight cyber crime*, 2011, online.

22 Robinson & Disley, *Incentives and challenges for information sharing in the context of network and information security*, p. 16. In addition to these 'high' importance incentives, they also identify 'medium' and 'low' importance incentives, including interpersonal trust, autonomy for participants with company support, and direct economic incentives, such as subsidies.

23 Yang & Maxwell, 'Information sharing in public organisations: a literature review of interpersonal, intra-organisational and inter-organisational success factors', p. 169. Interestingly, they find intra-organisational sharing more problematic than intra-organisational sharing.

24 M-E LeBeuf , S Pare, *Police information sharing in Canada: balancing security, efficiency and collaboration*, Royal Canadian Mounted Police, Ottawa, 2005, p. 23.

25 Discussion with Australian Government official, 23 May 2016.

26 For a significant criticism concerning the inability to aggregate and make sense of existing information holdings by government, see National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission report*, 2004, pp. 353–357, online.

27 One interlocutor spoke highly of the US PATRIOT Act sections 314(a) and 314(b), which help law enforcement identify, disrupt and prevent terrorist acts and money-laundering activities by encouraging further cooperation among law enforcement, regulators and financial institutions to share information about those suspected of being involved in terrorism or money laundering (see FinCen's 'Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act', online and FinCEN's 314(a) Fact Sheet, online).

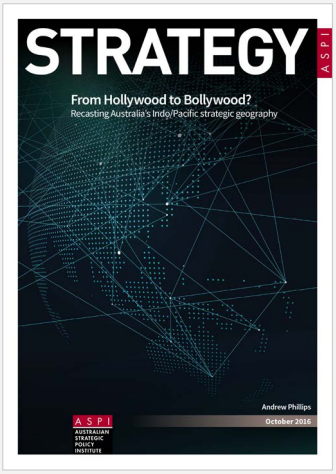
28 A view (now dated) expressed in National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission report*, p. 79, online. Still, information gained through electronic surveillance under 50 US Code § 1806—'Use of information' can't be disclosed to law enforcement 'unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General' (section b).

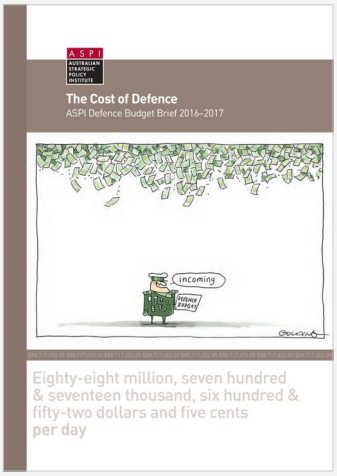
29 See Cabinet Office, *Government security classifications*, HM Government, April 2014, which says that officials need to share information proactively (para. 8) and are subsequently required to share only with those who have a 'need to know' (para. 9). Note the impassioned plea for officials to adopt a 'need to share' approach contained in *The 9/11 Commission report*, p. 417.

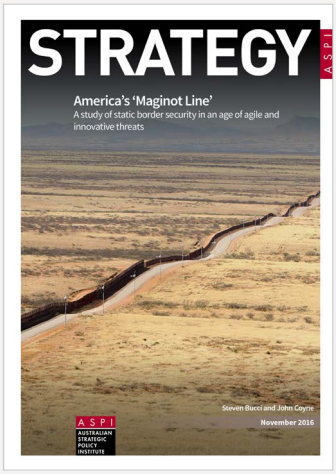
Acronyms and abbreviations

AML/CTF	anti-money-laundering and counter-terrorism financing
DCPCU	Dedicated Card and Payment Crime Unit (UK)
ECTF	Electronic Crimes Task Force (Netherlands)
FBI	Federal Bureau of Investigation (US)
FFA UK	Financial Fraud Action United Kingdom
IP	internet protocol
NFP	not for profit
NYPD	New York Police Department
UK	United Kingdom

Some previous ASPI publications







For the right reasons, in the right ways (Part 1)

A four-nation survey of information sharing about organised crime

ISSN 2200-6648