RULES IN INFORMATION SHARING FOR SECURITY

JANET CHAN, SARAH LOGAN AND LYRIA BENNETT-MOSES

Forthcoming (2020) Criminology and Criminal Justice
[2020] *UNSWLRS* 78

UNSW Law
UNSW Sydney NSW 2052 Australia

Rules in information sharing for security (8854 words)

Janet Chan[1], Sarah Logan[2] and Lyria Bennett Moses[3]

Published version available online: Criminology and Criminal Justice, DOI:

10.1177/1748895820960199

Abstract

Information sharing has become a central concern for security agencies since 9/11. Previous research has identified a number of barriers to information sharing among agencies: a combination of legal or policy constraints, interagency rivalry and mistrust, and technology. Drawing on ideas from the sociology of information and trust, this article conceptualises the sharing/withholding of information between agencies as

[1] Co-leader, Data Justice Research Network, Allens Hub for Technology, Law and Innovation and Professor at the Faculty of Law, UNSW Sydney. Janet is a multidisciplinary scholar with interests in occupational cultures, policing and the use of technology in criminal and social policy. Email: j.chan@unsw.edu.au, telephone: +61 401 713 461.

[2] Lecturer, Department of International Relations, Coral Bell School of Asia Pacific Affairs, the Australian National University. Sarah's research focuses on the international politics of information technology. Email: sarah.logan@anu.edu.au, telephone: +61 2 6125 5111.

[3] Director, Allens Hub for Technology, Law and Innovation and Professor, Faculty of Law at UNSW Sydney. Lyria's research addresses the relationship between technology and law, legal issues associated with the use of artificial intelligence techniques, and governance of law enforcement intelligence practices. Email: lyria@unsw.edu.au, telephone: +61 2 9385 2254.

dependent on rules as a system of trust. Adapting Richard Ericson's framework of the different contexts of rule-following and making use of an Australian case study, the article demonstrates how law, culture and technology are intertwined in constraining or enabling access to information. The implications of this model for legal and policy interventions are discussed.

Keywords: information sharing, security agencies, rules, trust

1. Introduction

Information[4] sharing has become a central concern for security agencies since 9/11 (Jones, 2007). Increasingly, task forces and public inquiries have called for agencies to facilitate greater data sharing in order to improve efficiency and effectiveness in the face of serious security threats (e.g. Parliamentary Joint Committee on Law Enforcement, 2013; Markle Foundation, 2006). For security agencies, data sharing has been regarded as crucial for meeting the challenges of globalised threats of terrorism, the transnational attacks of cybercrime, and the organised nature of serious crime (Jenkins, Liepman and Willis, 2014; Nolan, 2015; Brown, 2018). Yet the reluctance of

[4] In this article we use the term "information" and "data" interchangeably as unprocessed as well as processed material that may be analysed to form "intelligence" (Brown 2018:2; more generally, see Ratcliffe (2016: Chapter 5) on the DIKI (data, information, knowledge, intelligence) continuum.)

agents to share information has long been a problem documented in the policing literature (Chan, 2003; Sheptycki, 2004; Sanders, Weston and Schott, 2015; Taylor and Russell, 2012; Brown, 2018). A variety of "barriers" to data sharing have been offered: technology, funding, governance and policy, the business models of technology providers (Hollywood and Winkelman 2015), legal constraints, a sense of ownership, interagency competition and mistrust (Chan and Bennett Moses, 2017; Brown, 2018), organisational structure and culture (Abrahamson and Goodman-Delahunty, 2014; Glomset et al., 2007). However, as Jones (2007) points out in relation to national security intelligence, there are flaws in the underlying logic and the implementation of a presumption in favour of information sharing: a larger flow of information does not always make agencies "smarter", it is equally possible to overwhelm the capacity of agencies to separate the signals from the noise and lead to inappropriate responses.

This article aims to clarify the dynamics of information sharing through a conceptual model drawn from the sociology of information that sees the sharing and withholding of information as contingent on *rules* as a system of trust. To conceptualise how decisions about information sharing can be dependent on rules, we draw on Richard Ericson's (2007a) framework that examines the myriad contexts of rule-following in policing: the following of formal rules, exercising discretion, drawing on cultural

knowledge, complying with communication formats, and operating without rules. We adopt Ericson's conception of rules which includes legislation and other recognised sources of law as well as formal bureaucratic or administrative rules promulgated within particular agencies but excludes rules of thumb derived from police culture (Ericson 2007a: 370-372). Synthesising this literature, we postulate that information sharing in an age of datafication is a practice that depends on the interaction of formal rules, culture and technology. We make use of an Australian case study that uses technology to facilitate data sharing (see Section 3) to demonstrate how formal rules, culture and technology are intertwined in constraining or enabling access to information (Section 4). The implications of this model for legal and policy interventions are discussed in the concluding section.

2. Conceptualising rules in information sharing

Secrecy

Instead of focusing on information sharing, we find it useful to draw our initial inspiration from the sociology of secrecy. Simmel's (1906) paper, from which subsequent work by others have developed, posits that knowledge and secrecy are both central to social relationships. While having some knowledge of the other person is the precondition of a relationship, it is impossible to know everything about the

person. At the same time, this partial knowledge is often sufficient for social relationships to be formed. Simmel suggests that while the sharing of secrets in simple societies depends on direct knowledge about the trustworthiness of the receiver of the information, sharing in modern, complex societies needs to rely on a "credit-economy" or a system of trust (Simmel 1906:450). Marx and Muschert (2008) are among the first to link Simmel's paper to a sociology of information in the digital age (see also Soeters and Goldenberg (2019) for a recent reference to Simmel in relation to information sharing in multinational security and military operations). Marx and Muschert (2008: 221) argue that a sociology of information should emphasise the "structures, processes and consequences" of information control in different settings, including the "degree of symmetry with respect to the goals and resources of the interacting parties and the distribution of expectations regarding information". Without developing these ideas further, the authors offer a series of hypotheses for future exploration and empirical testing, one of which states: "The greater the development of information systems, the more behaviors related to information collection, processing, and communication will proceed from folkways and personal morality to mores, conventions, and laws (Münch)" (2008: 228, Table 3). In other words, Marx and Muschert (2008) have hypothesised that, with the advancement of information technology, the economy of trust in complex organisations is less

determined by individual values and personal relationships and more driven by cultural norms and formal rules.

Trust[5]

To clarify how rules operate to sustain an economy of trust for information sharing among security agencies, it is useful to examine the determinants of trust in organisations. Nooteboom and Six (2003:3) have suggested that "trust is associated with dependence and risk: the trustor depends on something or someone (the trustee or object of trust), and there is a possibility that expectations or hopes will not be satisfied, and that 'things will go wrong'.". Trust is not absolute, but conditional and contextual (2003:5). There are different bases for inferring reliability or trustworthiness: *characteristic-based trust*, which involves trusting someone on the basis of their membership in certain family, community or culture; *institutions-based trust*, which relies on rules, ethics, or professional standards to infer trustworthiness; and *process-based trust*, which is premised on loyalty, commitment and routinisation (Nooteboom, 2003:23). This kind of analysis is helpful for understanding how decisions about the sharing of information can be dependent on rules or norms that

[5] There is a considerable volume of literature on public trust in the police (e.g. Goldsmith 2005; Murphy et al. 2014). This literature will not be discussed here as we are more concerned with trust between security agents and agencies in decisions related to information sharing.

organisations have developed about the trustworthiness of the potential recipients of information, e.g. whether certain groups or organisations are deemed reliable, whether there are rules or standards that can ensure reliability, and whether the processes have proved reliable in routine information sharing.

Rules

To gain further insights into the relationship between rules and information sharing, we examine the wider question of how rules relate to security practice. Ericson has written extensively about rules in policing, drawing on both theoretical/philosophical writings on rules and empirical studies of policing in Anglo-American jurisdictions (e.g. Ericson, 1981, 1982, 2007a,b; Shearing and Ericson, 1991; Dixon, 1997). In Ericson (2007a:367), he integrates insights from this literature to put forward five perspectives on "how rules relate to police power and discretion". By capturing different types of rules, including the absence of rules, involving both a top-down and a bottom-up viewpoint, these perspectives provide a useful framework for analysing the different contexts in which trust develops. Ericson labels these perspectives as (i) following the rules, (ii) using the rules, (iii) beyond the rules, (iv) within the rules, and (v) without the rules. We will explain each of these perspectives briefly and anticipate how they can

inform our understanding of how rules relate to information sharing in security agencies.

i. Following the rules

The existence of rules can promote trust. Formal rules, in particular, "ensure a predictable environment in which to make rational choices about rule-governed behavior" (Ericson 2007a:368). In the context of information sharing in Australia, formal rules (and, in particular, law) designate whether information can be shared, to whom, and under what circumstances. They also provide a basis for withholding information (e.g. Chan and Bennett Moses, 2017). This suggests that formal rules can be limited as a tool for inferring trustworthiness.

ii. Using the rules

This perspective recognises that discretion is part of how policing agents enforce formal rules and follow procedure. In criminal law, for example, police typically enjoy wide discretion in whether to enforce the law and in how to justify the legitimacy of their actions (Dixon, 1997; Ericson, 2007a). In the context of information sharing, it is often the case that terminologies are confusing and rules regarding sharing complex or vague (Bennett Moses, 2020), so that security agents need to use discretion in

interpretation and in adopting informal procedures. The use of discretion (which differentiates using rules from following them) implies that security agents cannot rely on formal rules alone to assess the trustworthiness of the recipient of information, but will need to infer reliability based on the characteristics of the recipients or processes that have been routinised.

iii. Beyond the rules

This perspective emphasises the importance of embodied cultural knowledge in security decisions. Rules are made sense of through security agents' own experiences and the "war stories" told by veteran policing agents: "These stories are case studies thick with strategies: ways of seeing, being and acting as a police officer in different situations" (Ericson 2007a:377). When applied to information sharing, this perspective emphasises the importance of cultural norms or institutionalised practices for inferring trustworthiness.

iv. Within the rules

This perspective uncovers the generally hidden fact that rules are increasingly embedded in communication formats such as bureaucratic forms, fields in digital information systems and standardised reports. These can be seen as part of the push

towards managerialism and accountability in organisations (Ericson, 2007a). In the context of information sharing, trustworthiness is built into the communication format or even automated into the process of sharing.

v. Without the rules

This final perspective suggests that rules of security work are increasingly reconfigured through "counter-laws" which "negate the traditional principles, standards and procedures of criminal law" and involve the expansion of pre-emptive strategies and surveillance networks (Ericson 2007a, p.387; Ericson, 2007b). The threat of terrorism and the ubiquity of sensing devices have resulted in certain agencies (or some agencies under certain circumstances) to be exempted from privacy or other due process rules. When applied to information sharing, this is the opposite side of the first perspective and an extension of the fourth perspective: the absence of formal rules opens the gates to the free flow of information, while the expansion of sensing/surveillance networks automates the process of information flow.

A model of information sharing

These five perspectives capture the range of contexts in which trust develops and trustworthiness is evaluated in relation to information sharing. To sharpen our

analysis, we will group Ericson's five perspectives into three elements to be explored: (i) *formal rules* which includes "following the rules", "using the rules" and "without the rules", (ii) *culture* which represents "beyond the rules", and (iii) *technology* (rules embedded in communications formats) which Ericson refers to as "within the rules". These represent three inter-related structures upon which a trust economy for the management of information develops. These relationships are schematised in Figure 1. A brief explanation of these three elements and their interrelationships will follow.

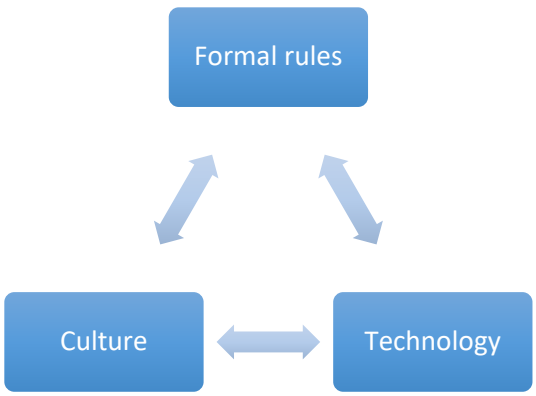

Figure 1: Three structural bases for trust in information sharing

Formal rules

Formal rules—in the form of laws, regulations or standard procedures—constitute a type of institutions-based trust (Nooteboom, 2003:23). Law plays a particular role in setting rules for information sharing because it applies to transactions between rather than within agencies and involves significant penalties (including jail) for non-compliance (Bennett Moses, 2020). It can impose constraints as well as generate resources for information sharing in security work: legal rules can prohibit one agency from sharing data with another agency or create exemptions so that an agency can obtain data not available to others. In general, law can enhance the power of certain agents or agencies or limit their discretion by imposing a higher level of accountability. The presence of formal rules as promulgated by legitimate institutions narrows the conditions and contexts in which trustworthiness can be inferred and information sharing facilitated. However, formal rules are not all clear-cut; they are subject to interpretation or in some cases can be bypassed.

Culture

Culture—in the form of shared tacit and embodied organisational knowledge among agents[6]—constitutes a form of "process-based trust" (Nooteboom, 2003:23). Information sharing is a social practice shaped by this kind of assumed knowledge. For example, ideas about reciprocity, compensation and transfer of ownership may be present, as may expectations about the extent to which individuals can legitimately claim or enforce control of information once it is shared. These expectations constitute a "system of trust" which allows security agents in a complex world to ascertain confidence in their knowledge of another individual and their agency which then facilitates sharing instead of withholding information.

Technology

Technology—in the form of automated and standardised "communication formats" (Ericson, 2007a:380)—constitutes another form of "process-based" trust (Nooteboom, 2003:23). Knowledge management infrastructure has become increasingly integrated (Hughes and Jackson 2004: 70-73), embedding rules regarding information sharing. For

[6] There is a vast literature on how culture is defined and conceptualised; in this article, culture is conceived as "figurative action" (Shearing and Ericson, 1991), so that action takes place "within a habitus of embodied knowledge (Bourdieu, 1962; Taylor, 1992)" (Ericson, 2007a:378). See also (Chan, 1997; 2003) for further elaboration of the relationship between police practice and embodied knowledge.

example, some rules for data access are routinely built into computer systems so that passwords or appropriate security levels are required to obtain clearance. Similarly, computer systems can be designed to facilitate the sharing of data between agencies but in practice often prevent extraction of data in useable formats. Coercive systems can be designed so that it is mandatory for certain information to be entered and procedures are difficult or impossible to bypass (Ericson and Haggerty, 1997).

Interrelationships among formal rules, culture and technology

These three elements do not operate independently. There is considerable empirical support that advances in information technology have affected both the structure and the culture of policing by introducing new formats for communication, limiting discretion and increasing transparency (Manning, 1996; Ericson and Haggerty, 1997; Chan, 2003). Information technology can also be used to monitor police performance, maintain audit trails, or implement accountability requirements (Chan, 2003). Culture, in the form of "technological frames" (Orlikowski and Gash, 1994) adopted by security agents, can affect how technology is designed and used (Chan, 2003; Chan and Bennett Moses, 2017). In our case study we will examine the extent to which and how these interrelationships may affect information sharing.

3. Research methods

To explore the role of formal rules, culture and technology in shaping information sharing practices, we draw an Australian study carried out in April to July 2017 among law enforcement agencies[7]. Three research methods were adopted: analysis of Australian federal and State legislation relevant to information sharing, semi-structured interviews and focus groups with policing agents. The research was carried out in the context of a new system for information sharing between agencies, the National Criminal Intelligence System (NCIS)[8], which was being trialled at the time. The focus of the project was to identify the legal and regulatory, as well as elements of organisational culture and practice within policing agencies, that might impede the sharing of data.

[7] The project was approved by the [University] Human Research Ethics Approval Panel on 4 January 2017 (Reference number: HC16972).

[8] The NCIS was designed to operate in a "secure, national information sharing environment", to "support collation and sharing of criminal intelligence and information across state, territory and Commonwealth law enforcement" (https://www.acic.gov.au/ncis). Although the word "intelligence" is included in the NCIS, the terms "information", "intelligence" and "data" were generally used without distinction in the project brief, as the focus was on the sharing of digital information which may or may not have been labelled as intelligence. We also asked interview participants how they might distinguish between the three concepts. The majority saw information and data as similar (although data is often associated with digital technology), but information can be turned into intelligence through assessment and analysis to provide insights and "add value" to the understanding of a problem.

Legal analysis

As explained above, legal rather than bureaucratic rules are most relevant when considering how information is transferred between (as opposed to within) law enforcement agencies. There is no one law that governs transfer of information to law enforcement agencies in all circumstances. Rather the applicable law will depend on the nature of the information concerned, the agency currently holding that information, the jurisdiction in which that agency is located within Australia, and the jurisdiction in which the law enforcement agency is located. In particular, there are a variety of database-specific and agency-specific laws concerning data transfer, in addition to the fact that Australia comprises a federal jurisdiction, six state jurisdictions and two mainland territory jurisdictions. We confined our legal analysis to the federal jurisdiction, New South Wales and Victoria. Within these jurisdictions, we focussed on general laws regulating data privacy and law enforcement agencies as well as a sample of laws regulating specific data sets. The purpose was not to obtain a comprehensive picture, but to understand the range of laws relating to specific datasets or specific data-holding agencies. The legal analysis is accurate as at 31 August 2017, and reflects the law at the time of the interviews. Not all intra-agency bureaucratic rules are publicly available, but the analysis included publicly available guidelines and other relevant documentation.

Interviews

A purposive sample was selected of research participants who had relevant knowledge of and expertise in the usage, classification, sharing and management of data within the context of the NCIS. To obtain a cross-section of participants, a total of 31 semi-structured interviews were conducted with staff currently or formerly associated with State or Federal police forces, criminal intelligence or other Federal law enforcement agencies, from very senior (about 40%) to operational staff (about 60%). Participants were asked questions regarding their information sharing practice, perceived barriers to information sharing and options for overcoming barriers.

Recruitment of interviewees was facilitated by the Australian Criminal Intelligence Commission (ACIC) which provided contact details of potential research participants from relevant agencies. Researchers recruited participants by sending email invitations together with copies of consent forms. Twenty-three interviews were conducted in person, and eight by phone, after receipt of written consent. Three were transcribed live; the remainder were recorded with permission and transcribed subsequently. Interviews were conducted between 17 April and 26 May 2017. Participation in the interviews was voluntary, the identities of all research participants are kept

confidential. To maintain confidentiality of information related to the sponsoring agency, this recruitment and interview process was conducted by a member of the project team cleared as a temporary member of the ACIC.

Focus groups

A total of 30 participants took part in five focus groups conducted in Canberra, Melbourne and Sydney between May and November 2017. Group size ranged from four to eight. The participants form a purposive sample that represent several law enforcement agencies. Public service participants were mid-ranking, and sworn police participants were between the rank of Sergeant and Chief Inspector. The discussion topics included participants' perceptions of the benefits and risks of two main reform options for improving information sharing identified by interview participants: law reform and cultural change. Participants were also invited to suggest other reform options.

Focus group participants were chosen on the basis that they had relevant knowledge of and expertise in the usage and management of data within the context of a specific data-sharing platform NCIS. Recruitment of interviewees was facilitated by the ACIC which provided contact details of potential research participants from relevant

agencies. Researchers recruited participants by sending email invitations together with copies of consent forms. Participation in the focus groups was voluntary and transcripts were anonymised as above.

Empirical data analysis and limitations

Analysis of the interviews and focus groups data involves coding participants' responses thematically using prior concepts as outlined above as well as being open to the discovery of new concepts. All coding was carried out by [the second author] who also conducted all the interviews and most of the focus groups.

Given that the samples of 31 interview participants and 30 focus group participants were not randomly selected to be representative of the population of law enforcement staff, findings of this research provide a good indication of the issues, concerns and opinions relevant to the project, but they do not necessarily represent the full range of views in this population. Note also that where legal and regulatory issues were mentioned in focus groups, the information was interpreted as reflective of research participants' *perceptions* rather than doctrinal accuracy.

4. Information sharing: The role of formal rules, culture and technology

This section highlights the findings of the legal analysis and the interview component of the study. We will use the model in Figure 1 to organise the results, i.e. the extent to which formal rules, culture and technology constrain or facilitate information sharing among security agents.

Formal rules

To understand the role of formal rules in promoting trust and setting out rules for information sharing, we examined current laws and regulations and publicly available bureaucratic rules as well as analysed the views of interview and focus group participants.

Restrictions on the flow of information can be justified by a range of reasons, e.g. the presence of ongoing policing operations, sensitivity of certain types of information, security classification, privacy, and so on (D2D CRC, 2017:19). An analysis of current laws and regulations governing data sharing suggests that in Australia there is a "patchwork of legal rules for different datasets, agencies and jurisdictions contributing to a complex, confusing and restrictive legal framework." (D2D CRC, 2017:5). For example, strict rules govern the disclosure of information and documents held by the Australian Customs Service; AUSTRAC data; identifiable taxation information;

migration data; protected social security information; health information. The volume of restrictions is problematic because it requires the "navigation of multiple laws to determine what information can be requested by an officer from one agency and from which agencies that request can be made" (D2D CRC, 2017:5).

The complexity of legal rules is compounded by a number of issues that are specific to certain circumstances. For example, there may be restrictions in disclosing information to other agencies for law enforcement purposes. These restrictions may mean that "disclosure can only occur *after* an offence has been or may have been committed" or that "disclosure cannot be made for the purposes of *investigating* an offence" (D2D CRC, 2017:6). Further, legislation that allows disclosure of information often applies for the purposes of that particular legislation only, limiting the possibility of on-sharing that information for other purposes or to other entities. This suggests that the complexity of legal rules could multiply when multiple sources are relied on in an intelligence product (D2D CRC, 2017).

There are a variety of other rules-based challenges for information sharing. Administratively, information sharing often requires authorisation from senior officers. The status of data matching varies by jurisdiction, with only *some* jurisdictions offering

the ability to have data-matching programs authorised through following guidelines. Where there are guidelines, these may be difficult for law enforcement agencies, for example requiring notification of the public (Office of the Australian Information Commissioner, Guidelines on Data Matching in Australian Government Administration (June 2014), Guideline 5). Further, diverse terminology is used in federal and state legislation to connect particular data, information or records with a particular agency (Bennett Moses, 2020). The result is that determining *which* agency-specific legislation is relevant is itself potentially complex, particularly where data is not clearly within the control of a single agency, as in the case of cloud computing and common data platforms.

There are thus various ways in which the legal framework around information sharing in Australia is both complex and inconsistent. These include federalism (which creates different rules in different jurisdictions), proliferation of rules that apply to specific agencies or specific datasets, and important differences among the rules that might apply including in relation to terminology (with more than one set of rules applying to a document collating information from different sources). However, none of this suggests that rule-following will *necessarily* be difficult or onerous in all circumstances.

Nevertheless, because compliance with data sharing procedures is required *before* it can be ascertained whether useful information is revealed, law is often perceived as a barrier. In particular, the law does not only constrain the sharing of *substantive* information, but also metadata about information held by particular agencies. For example, disclosing the fact that there is an entity "John Smith" in a database is a "disclosure" despite the fact that no information about John Smith is revealed.

The above findings are consistent with the perceptions of research participants who took part in interviews and focus groups. When asked to identify barriers to information sharing, most participants mentioned the complexity of rules and procedures as an example. A sizeable proportion of interview participants focused on the complexity of disclosure rules and processes *between* organisations which were a significant source of frustration for participants:

> … our legislation at the moment and other government policies present obstacles to information sharing. Most information collected by a government entity is collected under a certain legislation … that can prevent [one organisation] … sharing that data with … [another organisation] or with somebody else … unless there's been special legislation made that permits that.

> [NCIS manager]
>
> when different packets of information and different powers are treated on their own terms [barriers to information sharing are] the natural consequence. [NCIS manager]

The time taken to "get signed off on by a manager or point within the agency", including in some cases "across our legal department and then final signoff via a national manager or delegate of a CEO" was mentioned as playing a simultaneous role as barrier and protection.

Inconsistency in legal framework was also cited as a barrier to information sharing. Apart from the complexity and inconsistency of formal rules, participants pointed out that even administrative rules require interpretation. The concept of "need to know" was cited as one rule that is susceptible to different individual interpretations:

> … my version of need to know and your version are going to be different … [B]ecause everyone has different tolerances. [NCIS user, police officer]

Participants described different ways to "get around" the problem of access by using existing rules creatively. For example, establishing personal relationships or networks was one way to gain access to information "legitimately":

> …between agencies there are official channels and unofficial channels of getting information. That can be difficult until you have established a network and you can legitimately share information. It is an easier process once you have established a relationship rather than trying to go through the proper channels. You create networks and you learn how to get information. [NCIS user, police officer]

Some participants noted that members in a joint-agency collaboration were sometimes used as information sources:

> [Joint operation] is a real mixing pot. …they can just ask the guy who is sitting there, "Hey, can I have that information?" And, of course, the efficiencies gained from that are huge. [Police executive]

The presence of liaison officers in some units was an effective way of facilitating data sharing:

> …you don't have to do an RFI [Request for Information] form – you just walk across the floor or pick up the phone or just write in an email…[NCIS user, police officer]

One participant went as far as suggesting that legal issues were the "showstopper because that will inform your security framework and your IT framework as far as how you manage the data in that environment"; for this participant, the "natural default" to refuse to share information was caused by the complexity of the legal framework [Police executive].

Focus group participants were asked their views on law reform—through standardisation of legislation, simplifying the rules of disclosure, and separating discoverability from disclosure—would make a difference to information sharing, and whether there are any risks involved.

Standardising legislation. Participants were generally positive about standardising legislation. They saw benefits for sharing with international agencies; for simplifying disclosure chains, where intelligence in an analytic report must be disclosed by originating agencies; for making parliamentary intent clearer, easing the burden of interpretation. However, participants also raised concerns such as the difficulty of standardising terminology around different datasets with complex sensitivities and the potential risks of extending federal legislative standardisation to State agencies because of the "flow-on effect" which might lead to resistance. Others argued that even given standardisation, inconsistent interpretations and lack of management systems to support standardisation could still change the outcomes. As one participant pointed out, standardisation is only one step, it is not going fix everything, but it is a necessary step.

Simplifying disclosure. Participants were asked about the idea of having individuals determine the sensitivity of a piece of information when they enter it into the system, instead of agencies making that decision only in response to requests for information, (RFI), as was currently the case. Some already had such a system. However, the appropriateness of the decision would depend on the experience or knowledge of the agent entering the data: inexperienced officers might over- or under-classify the

information. Participants also identified several risks to reforming disclosure in this way: first, investigators might hoard the information and not release it to anyone or over-classify it so that it remained within the agency; secondly, if sensitive information was added subsequently to the initial entry, the dissemination code might not be changed to reflect the new status. This means that context is important for making decisions about information sensitivity, and context can change, so that the aggregate of different pieces of information could change the value and sensitivity of information which might not seem important at the point of collection. Classification levels might also change over time, necessitating a review of initial classifications. Other participants noted that simplifying disclosure would work with standard information, but not necessarily with more complex or sensitive information.

Separating discoverability from disclosure. Participants were asked for their thoughts on the benefits and risks of distinguishing between discovery and disclosure. Creating a master index of entities on which information is held makes the fact that information is held on those entities "discoverable". This is, potentially at least, limited by rules restricting disclosure of information. The idea was to have fewer restrictions on discoverability than on disclosure so that users of the system will know whether there is information out there on a person or entity they are interested in, and they will

know where the information is held, but they may need to follow ordinary request procedures to obtain the information itself. A number of participants saw such a system as helpful in saving time while adhering to the “need to know” principle. However, participants noted that such a system might involve risks to data security, data quality, loss of context, slow or inconsistent disclosure process, and making inadvertent or undesirable disclosures.

In sum, both our legal analysis and interview data support the conclusion that while legal rules and regulations can theoretically provide a predictable environment for information sharing, the current complexity and inconsistency of these rules in Australia fail to provide the necessary guidance for information sharing. Security agents often have to resort to personal network or relationships to “work around” the problem (cf Cotter, 2017). Focus group data points to problems and risks inherent in law reform which cannot anticipate all the contingencies and sensitivities of data sharing practice.

It should be noted that our legal analysis found that there are certain exemptions that apply to accessing data for law enforcement purposes. However, this enabling aspect of formal rules was not mentioned by any research participants. This suggests that

when rules were not seen as a problem for data sharing, participants were unlikely to mention any exemptions they enjoyed. Participants also did not mention the use of data for mass surveillance as pointed out by Ericson (2007a). This is consistent with our finding that security agents we interviewed were mainly concerned with using data for operational intelligence in relation to case-based criminal investigations, prosecutions or disruptions, where access was normally for data with individuals being identified; none mentioned the use of big data or predictive analysis, although a few suggested that data was used for tactical or even strategic intelligence.

Culture

To understand the influence of cultural knowledge and expectations on building trust and promoting the sharing of information, and the prospects of cultural change as a reform option, we draw on the interview and the focus group data.

Most interview participants mentioned “culture” as a barrier to information sharing. When we probed further into what participants meant by “culture”, we found a variety of words that were used in discussing culture. For example, culture was discussed in terms of customs, practices or routinised ways of doing things; mindset; “who we are”; or beliefs, attitudes, “natural disposition”. Most regarded culture as a useful term,

especially in relation to organisational culture, but some participants pointed out the existence of multiple cultures within an organisation. When discussing culture as a barrier to information sharing, some participants emphasised the importance of "trust" or "credibility" which has to be "earned" or "built up". Aspects of culture that impede information sharing were: protectionism, risk averseness, competitiveness, and secrecy.

Nevertheless, participants indicated that organisational cultures were changing and were no longer the main barrier to information sharing. Indeed, despite several noting that organisational competition did play a role, a substantial number noted that they considered their experience of information sharing to be positive, or at least as having changed for the "better":

> I think culturally we are getting closer [to] what we need to with sharing that information. It is becoming less of an issue, especially when we are seeing all these larger events or terrorist activity or so on. The recognition that we need to be able to share this information quickly is becoming more prominent and widely accepted, I would say. Certainly, I think there has been a mindset shift if

> not a cultural one….I think individuals still have trouble but I think organisations are getting there. [Police executive]

Several participants acknowledged that cultural barriers continued to exist, with some "pockets" of culture still resistant to sharing. However, they were more likely to describe the barriers as resting with individual attitudes than organisations as a whole. Some noted that reluctance to share data could be the result of a risk-averse mindset or culture:

> There is definitely a culture of where people want more levels of approval, just in case. It is always in the back of the mind to be cautious when sharing anything and take the appropriate steps. [Police executive]

One participant admitted that over-classification of information was "one of our biggest problems, where we are hiding information from ourselves". Another participant pointed out that understanding "how the system works" can be important for making sure that information is made available to others by using the lowest level of classification. Thus, informal rules that form part of police cultural knowledge are not necessarily impediments, they can often serve to facilitate data sharing.

Two aspects of cultural change as a reform option were canvassed in the focus groups: training and leadership.

Training. Some participants agreed that more training was generally a good thing as it can build trust in a system and facilitate the development of rapport across agencies. However, individuals still had to make decisions about whether or not to share information, and training would not guarantee they would make the right decision. Several suggested that tailoring training in general was very difficult; it often needed to target individuals who might be too senior to have time to attend. Given the variation across organisations, training was said to be too complex to manage. Two participants noted that training was ineffective without leadership, emphasising the importance of broader organisational factors such as systems design and the demographics of organisational members.

Leadership. Some participants agreed that leadership in general was important to improving information sharing. However, leaders needed to be supported in driving change: they are not likely to take risks unless "they are comfortable that there isn't a zero tolerance for failure". Several participants noted that senior leadership in their

agencies was already committed to information sharing, but that middle management could block relevant initiatives. This layer of management was described as "permafrost" which is difficult to break through. One participant noted that leadership stability or continuity was valuable for retaining institutional knowledge and leadership accountability.

*Other options***.** Several participants emphasised the benefits of improving interagency relations as a way to build rapport and improve information sharing. It was suggested that the incentives offered to individuals for sharing information should be addressed. Participants noted that while responding to Requests for Information (RFI) was a significant part of their workload, it was not recognised by management: "You don't get rewarded for doing an RFI and you only get punished for not finishing your own work". Some participants suggested that incentives would not work but the automation of information uploads appeared to solve the problem.

In sum, the interview data suggests that security agents agree that information sharing is to be encouraged (cf Jones 2007) and that "culturally" they have become more willing to share information. To be sure, there are "pockets" of culture and some

individuals who hold a “risk-averse mindset”, but there is a sense of optimism that knowing “how the system works” can get around some of the obstacles to sharing. Focus group data shows that agents are equivocal about organisational change as a reform option as it can be complex and not necessarily effective for improving data sharing.

Technology

To investigate the role of technology in building trust and promoting the sharing of information, and the risks and benefits of technological tools as a reform option, we again draw on the interview and the focus group data.

Interview participants were asked directly whether the data-sharing platform NCIS had helped to address some of the barriers to information sharing they had identified. Almost all said yes, with others saw the NCIS as only a start. The platform had overcome some of the complexity of disclosure identified earlier:

> Once the NCIS – if it gets up and running – there will almost be an assumed MOU [Memorandum of Understanding] for want of a better word. If an agency

> has placed their data in the NCIS it will be assumed they want to share. I think it will go a long way to breaking that [barrier] down…[NCIS user, police officer]

Most interview participants who had used the platform were extremely positive about it. As one participant put it: “build it and they will come”. The availability of the system could break down some of the cultural barriers:

> I think it lets people see what the dividends of information sharing are. [NCIS user, police officer]

> …[If] they are that deadset against it then you are never going to change it because it is a personal thing. But if that person is surrounded by 20 people who are progressive and like working with others, and they like working in the joint space they will go to that baseball field and work well together and get results. [NCIS user, police officer]

Focus group participants discussed ways in which technology could be used to great effect as a reform option. For example, the use of metrics of system usage and analytics could improve information sharing: “Just having some data analytics around

the how the information is used, how often it is used, who is using it, who is not using it, so that you can obviously try and identify issues". This requires updating old systems and getting the right technology in place, which is even more important in the context of large volumes of data now being generated, so that it is not possible to go through the data manually. Other suggestions include: having a "smart system" that could interpret requests and provide a ranking of information, automation as a way to ensure information was loaded into the system, or making disclosure automatic when the seeker of information is authorised to receive it. It was suggested that providing an audit trail would allow managers to enforce accountability for information sharing. One participant suggested that such an audit trail could also help provide incentives for information sharing by improving attribution: "knowing that your intel was accessed, used, relevant for some purpose" could be "a great incentive". Auditing or system-generated logs were seen as safeguards that could mitigate the risk of undesirable disclosures. Some emphasised that the use of automation was not to replace humans, which "is what keeps the trust alive".

In sum, the interview data shows that when data sharing is built into an information system, trustworthiness is assumed, as agents are no longer required to check legal rules for compliance and they are optimistic that the existence of such a system will

normalise information sharing as part of security practice. Focus group data suggests that technological tools could be effective for automating processes, enforcing accountability, and safeguarding risks in information sharing.

-:-

The above analysis shows how formal rules, culture and technology provide the contexts for the development of trust and the evaluation of trustworthiness when security agents make decisions about information sharing. In this Australian case study, we find that the complexity and inconsistency of formal rules (in particular, law) do not engender a sense of predictability and trust for information sharing; instead they have created real constraints that limit sharing. In contrast, agents seem to see the system of informal rules and expectations as moving towards a sharing culture, one that they have confidence in trusting and navigating within. Finally, agents are optimistic about and put a lot of trust in the ability of technological solutions such as the building of a data-sharing platform to overcome some of the legal and cultural barriers that impede data sharing. Noteworthy, too, is the interaction between formal rules and culture (such as overclassification, a way of using rules to limit information

sharing), and the use of technology (data sharing platform) to solve the problem of legal restrictions and to break down cultural barriers.

Our case study findings shed light on some of the interrelationships between formal rules, culture and technology. First of all, given the complexity and inconsistency of the law, agents need to rely on cultural knowledge to either interpret or bypass the law. We have less information on how law can influence culture, but it is possible that the proliferation of rules can lead to a risk-averse culture. Secondly, we see in the design of the NCIS that technology might eventually automate sharing within the rules, although we are not privy to the extent to which formal rules shaped the design of the NCIS. Finally, there are suggestions from the interviews that technology can also shape the culture of information sharing. We do not have direct evidence from this study that culture can affect the design and use of technology, but the literature on "technological frames" (Orlikowski and Gash 1994) has generated considerable evidence that cultural framing can influence how designers and users interact with technology.

5. Conclusion

Data sharing in contemporary society is a practice that has multiple and often competing meanings and political connotations. For example, sharing of information between security agencies and law enforcement, and in particular the mingling of intelligence and evidence, link criminal justice and covert powers in in ways that shift the power and boundaries between state and subject in problematic ways (McCulloch and Wilson 2016: 93-110). This paper does not argue that all information sharing is beneficial and it acknowledges that, at a practical level, the practice of information sharing between security agencies is multi-faceted. There are often good reasons for some agencies not to be totally transparent and their data universally accessible (see Bennett Moses and de Koker, 2017). In order to protect unauthorised access to data that might jeopardise current or ongoing investigations, information that is sensitive or private, or to ensure that due process is followed in criminal cases, a “patchwork” of laws have been enacted for specific agencies or types of data. It is obvious, to extend Simmel’s (1906) thesis, that knowledge and secrecy are both central to the relationships between government agencies. As organisations become larger and more complex, the policing of secrecy relies on an economy of trust.

Drawing on ideas from the sociology of information and trust, this article conceptualises the sharing/withholding of information between security agencies as dependent on rules as a system of trust. Following Ericson (2007a), this article opened up the possibility that processes for governing secrecy are not only found in law or formal rules, but also in culture or embodied knowledge, and technology or communications format. Our empirical results have suggested that formal rules, culture and technology are intertwined in creating constraints or enabling access to data that might otherwise be kept secret. In the Australian case study, the complexity and inconsistency in legal rules formed a formidable barrier to information sharing. In this situation, law does not provide a scaffold for building trust, although it may have served the purpose of security in some circumstances. Security agents, while supporting law reform as an option for clarifying rules and simplifying procedures, were nevertheless not entirely convinced that additional risks would not be introduced. Neither were they confident of organisational change as the way forward. Instead, they placed their trust on the building or maintenance of personal relationships and the use of technology to implement rules and bypass cultural resistance. Part of this trust in technology may have stemmed from their (positive) experience with the NCIS. The longer-term impact of law reform, cultural change and technological tools are yet to be tested. The findings of this case study may or may not

be unique to Australia. We would argue, however, that future research would benefit from a similar investigation of how the dynamic relationships between formal rules, culture and technology in specific settings can shape the practice of information sharing in organisations.

Acknowledgment

We thank all research participants, the ACIC, the Commonwealth Attorney-General's Department and especially Shannon Callaghan for facilitating this research project. We also thank David Dixon and Nofar Sheffi for their valuable comments on an earlier version of this paper. The authors declare that there is no conflict of interest.

Funding

This work was supported by the Data to Decisions Cooperative Research Centre (D2D CRC) [grant number DC52004].

References

Abrahamson, DE and Goodman-Delahunty, J (2014) Impediments to information and knowledge sharing within policing: A story of three Canadian policing organisations. *Sage Open* January-March 2014:1-17.

Adamson, FB (2005) Globalisation, transnational political mobilisation, and networks of violence. *Cambridge Review of International Affairs* 18(1): 31-49.

Bennett Moses, L (2020) Who owns information? Law enforcement information sharing as a case study in conceptual confusion. *UNSW Law Journal*. Forthcoming.

Bennett Moses, L and de Koker, L (2017) Open Secrets: Balancing operational secrecy and transparency in the collection and use of data by national security and law enforcement agencies. *Melbourne University Law Review* 41(2):530-570.

Brown, R (2018) Understanding law enforcement information sharing for criminal intelligence purposes, *Trends and Issues in Crime and Criminal Justice.* Canberra: Australian Institute of Criminology.

Chan, J (1997) *Changing Police Culture*. Melbourne: Cambridge University Press.

Chan, J (2003) Police and new technologies. In Newburn T (ed) *Handbook of Policing*, edn. 1, Cullompton: Willan, pp. 655 – 679.

Chan, J and Bennett Moses, L (2017) Making Sense of Big Data for Security. *British Journal of Criminology* 57(2), 299-319.

Cotter, RS (2017) Police intelligence: connecting-the-dots in a network society. *Policing and Society* 27(2):173-187.

Data to Decisions Cooperative Research Centre [D2DCRC] (2017) *Law and Policy Analysis (Report A) Project B2: Information sharing and the National Criminal Intelligence System (NCIS).* Unpublished report.

Dixon, D (1997) *Law in Policing: Legal regulation and police practices.* Oxford: Clarendon Press.

Ericson, R (1981) *Making Crime: A Study of Detective Work.* Toronto: Butterworths.

Ericson, R (1982) *Reproducing Order: A Study of Police Patrol Work.* Toronto: University of Toronto Press.

Ericson, R (2007a) Rules in policing: Five perspectives. *Theoretical Criminology* 11(3): 367-401.

Ericson, R (2007b) *Crime in an Insecure World*. Cambridge: Polity Press.

Ericson, R and Haggerty, K (1997) *Policing the Risk Society.* Toronto: University of Toronto Press.

Glomset, R, Gottschalk, P and Solli-Saether, H (2007) Occupational culture as determinant of knowledge sharing and performance of police investigations. *International Journal of the Sociology of Law* 35(2): 96-107.

Goldsmith, A (2005) Police reform and the problem of trust. *Theoretical Criminology,* 9(4):443-470.

Hollywood, JS, and Winkelman, Z (2015) Improving Information-Sharing Across Law Enforcement: Why Can't We Know? RAND corporation. Retrieved from www.rand.org.

Hughes, V and Jackson, P (2004), The Influence of Technical, Social and Structural Factors on the Effective use of Information in a Policing Environment. *The Electronic Journal of Knowledge Management* 2(1): 65-76.

Jenkins, BM, Liepman, A, and Willis, HH (2014) *Identifying Enemies Among Us: Evolving terrorist threats and the continuing challenges of domestic intelligence collection and information sharing.* Santa Monica: RAND Corporation.

Jones, C (2007) Intelligence reform: The logic of information sharing. *Intelligence and National Security* 22(3): 384-401.

Manning, PK (1996) Information technology in the police context: the "Sailor" phone. *Information Systems Research* 7(1):52-62.

Markle Foundation (2006) *Mobilising Information to Prevent Terrorism*, Third Report of the Markle Foundation Task Force.

Marx, GT and Muschert, GW (2008) Simmel on Secrecy. A Legacy and Inheritance for the Sociology of Information. In: Papiloud, C and Rol, C (eds) *Soziologie als Möglichkeit 100. Jahre Georg Simmels Untersuchungen über die Formen der Vergesell-schaftung* [The Possibility of Sociology: 100 Years of Georg Simmel's Investigations into the Forms of Social Organization]. Wiesbaden, Germany: VS Verlag für Sozialwissenschaften, pp217-233.

McCulloch, J and Wilson, D (2016) *Pre-crime: Pre-emption, precaution, and the future*. New York: Routledge.

Murphy, K, Mazerolle, L and Bennett, S (2012) Promoting trust in police: findings from a randomised experimental field trial of procedural justice policing. *Policing & Society*, 24(4):405-424.

Nooteboom, B (2003) The trust process. In: Nooteboom, B and Six, F (eds) *The Trust Process in Organizations: Empirical Studies of Determinants and the Process of Trust development.* Edward Elgar, pp16-36.

Nooteboom, B and Six, F (2003) Introduction. In: Nooteboom, B and Six, F (eds) (2003) *The Trust Process in Organizations: Empirical Studies of Determinants and the Process of Trust development*. Edward Elgar, pp 1- 15.

Nolan, A (2015). *Cybersecurity and Information Sharing: Legal Challenges and Solutions.* Congressional Research Service. Retrieved from www.crs.gov.

Orlikowski, WJ and Gash, DC (1994), Technological Frames: Making Sense of Information Technology in Organisations. *ACM Transaction on Information Systems* 12: 174 – 207.

Parliamentary Joint Committee on Law Enforcement (2013) *Inquiry into the gathering and use of criminal intelligence*. 15 May 2013. Commonwealth of Australia. https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/Completed_inquiries/2010-13/criminal_intelligence/report/index.

Sanders, CB, Weston, C and Schott, N (2015) Police Innovations, 'Secret Squirrels' and Accountability: Empirically Studying Intelligence-Led Policing in Canada. *British Journal of Criminology* 55: 711–729.

Shearing, CD and Ericson, RV (1991) Culture as Figurative Action. *British Journal of Sociology* 42(4):481-506.

Sheptycki, J (2004) Organizational Pathologies in Police Intelligence Systems: Some Contributions to the Lexicon of intelligence-led policing. *European Journal of Criminology* 1: 307–32.

Simmel, G (1906) The Sociology of Secrecy and of Secret Societies. *The American Journal of Sociology*. Xi(4):441-498.

Soeters, J and Goldenberg, I (2019) Information sharing in multinational security and military operations. Why and why not? With whom and with whom not? *Defence Studies* 19(1): 37-48.

Taylor, RW and 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.