



INFORMATION SHARING

(The role, if any, of s.8 of the Charter)

By: Michael Fawcett
Crown Counsel
Crown Law Office – Criminal

Michael Lacy
Brauti Thorning Zibarras LLP



WHAT IS “INFORMATION SHARING”?

“Information sharing” means the passing of information, sometimes personal in nature, from one arm of the government to another, either domestic or foreign.



THE TYPES OF INFORMATION SHARING



THE TYPES OF INFORMATION SHARING

Regulatory-to-Criminal: *R. v. Saikaley*



THE TYPES OF INFORMATION SHARING

The police identify Mr. Saikaley as a target in a major drug investigation. They know that he has left the country with his family on vacation and will be returning through the Ottawa airport. They write CBSA *via* e-mail and state:

“I just want to make sure that Mr. Saikaley is flagged and that anything he has on him is checked. As always, thanks a bunch! The RCMP”



THE TYPES OF INFORMATION SHARING

The CBSA in turn places a “lookout” on Mr. Saikaley’s file. It reads as follows:

“Subject of on-going criminal investigation. May be importing containers from overseas. Examine container and subject. Collect any intelligence electronic media, cell phone (subject known to have iPhone with documents within), contacts, recent calls, method of payment for trip, customs invoices, etc.”



THE TYPES OF INFORMATION SHARING

Mr. Saikaley arrives in Canada and, based on the “lookout,” a CBSA official directs him to secondary. Once there, an officer searches his luggage. The officer also searches Mr. Saikaley’s cell phone. The officer flips through the phone’s pictures and notices one of a large, brand new diamond ring. He then starts looking for an electronic invoice and discovers a “debt list.”



THE TYPES OF INFORMATION SHARING

The officer testifies – and the judge believes him – that he was acting with a *bona fide* customs purpose at all times.



THE TYPES OF INFORMATION SHARING

The CBSA makes a copy of the debt list and provides it to the RCMP. The RCMP uses it to get authorization for a Part VI. Through the wiretap, the police uncover Mr. Saikaley's large-scale drug operation. He is convicted and sentenced to 19 years. He appeals and alleges numerous section 8 violations.



THE TYPES OF INFORMATION SHARING

Criminal-to-Criminal: *R. v. Viscomi*; *R. v. Lane*



THE TYPES OF INFORMATION SHARING

Mr. Viscomi and Mr. Lane are alleged Internet predators. Both live in Ontario. Their crimes led to harms in both Canada and the United States.



THE TYPES OF INFORMATION SHARING

U.S. law enforcement learned about their online behaviour and advised Canadian police. Canadian police used what they learned to get search warrants to search the two men's Ontario residences and seize their computers. Canadian police were engaged in a *bona fide* domestic investigation at the time.



THE TYPES OF INFORMATION SHARING

The U.S. tells Canada that they want to prosecute Mr. Viscomi and Mr. Lane. The Crown stays the domestic charges and begins extradition proceedings. The U.S. then asks for the seized computers to assist their prosecution.



THE TYPES OF INFORMATION SHARING

Mr. Lane later challenges the domestic search warrant in the course of his extradition proceedings and succeeds. Mr. Viscomi does not raise a similar challenge. They both allege the sharing was improper.

REGULATORY → CRIMINAL: THE SECTION 8 CONCERN

Criminal

- The *Hunter v. Southam* criteria usually apply
 - RPG
 - Evidence under oath
 - Judicial pre-authorization

Regulatory

- No uniform constitutional test
- Permissive search powers:
 - No grounds
 - No need for evidence under oath
 - No judicial pre-authorization



REGULATORY → CRIMINAL: GENERAL RULES

Every section 8 analysis in the information sharing context is governed by two rules:

- (1) The *Bona Fide Purpose* Rule
- (2) The *Consistent Use* Rule

REGULATORY → CRIMINAL: THE *BONA FIDE* PURPOSE RULE

R. v. Jarvis, [2002] 3 S.C.R. 757

- CCRA receives tip that accused failed to report income from sale of art.
- Its business audit section uses its statutory powers to compel protection of information from accused.
- Auditor finds unreported income and possible fraud. Then, rather than completing the audit, the auditor refers the matter to Revenue Canada's special investigations unit for criminal prosecution.
- Shortly after the referral, bank records requested initially by the auditor also were forwarded to the investigator.



REGULATORY → CRIMINAL: THE *BONA FIDE* PURPOSE RULE

R. v. Jarvis, [2002] 3 S.C.R. 757

- Holding:
 - The auditor's regulatory super powers are not available to further a criminal investigation.
 - Where the “predominant purpose” of a particular inquiry is the determination of penal liability, CCRA officials must relinquish their regulatory super powers:
 - No further compelled statements
 - No further compelled production of documents
 - No documents produced for the predominant purpose of assisting the criminal investigation



REGULATORY → CRIMINAL: THE *BONA FIDE* PURPOSE RULE

R. v. Jarvis, [2002] 3 S.C.R. 757

- Holding:
 - To determine the predominant purpose of the regulator's inquiry and whether they have "crossed the Rubicon" to begin a criminal investigation, you look at a variety of factors, including:

REGULATORY → CRIMINAL: THE *BONA FIDE* PURPOSE RULE

R. v. Jarvis, [2002] 3 S.C.R. 757

Factors re: “Predominant Purpose”:

- Did the authorities have reasonable grounds to lay charges? Does it appear from the record that a decision to proceed with a criminal investigation could have been made?
- Was the general conduct of the authorities such that it was consistent with the pursuit of a criminal investigation?
- Had the auditor transferred his or her files and materials to the investigators?
- **Was the conduct of the auditor such that he or she was effectively acting as an agent for the investigators?**
- **Does it appear that the investigators intended to use the auditor as their agent in the collection of evidence?**
- Is the evidence sought relevant to taxpayer liability generally? Or, as is the case with evidence as to the taxpayer’s mens rea, is the evidence relevant only to the taxpayer’s penal liability?
- Are there any other circumstances or factors that can lead the trial judge to the conclusion that the compliance audit had in reality become a criminal investigation?

REGULATORY → CRIMINAL: THE *BONA FIDE* PURPOSE RULE

R. v. Jarvis, [2002] 3 S.C.R. 757

- Applying these criteria, the Court concluded that the regulatory tax documents and statements at issue in *Jarvis* were obtained by the audit unit for the predominant purpose of tax regulation, so their initial gathering and disclosure to the investigations unit did not give rise to a section 8 violation.



REGULATORY → CRIMINAL: THE *BONA FIDE* PURPOSE RULE

The *Bona Fide* Purpose Rule:

The search must be (1) authorized by law and (2) the predominant purpose of the search must amount to a *bona fide* exercise of that search power.

REGULATORY → CRIMINAL: THE *BONA FIDE* PURPOSE RULE

Hypothetical No. 1:

Accused is involved in a fatal car crash. The police suspect drinking and driving and begin an investigation. Meanwhile, the accused is transported to the hospital and a blood sample is taken for medical purposes. The Coroner seizes the sample pursuant to his powers as set out in the *Coroner's Act*. The Coroner then turns around and hands the blood to police to further their investigation, knowing the police wanted the sample and intended to use it in the criminal investigation.



REGULATORY → CRIMINAL: THE *BONA FIDE* PURPOSE RULE

R. v. Colarusso, [1994] 1 S.C.R. 20:

The warrantless seizure by police violated section 8 as police should have obtained a search warrant.



REGULATORY → CRIMINAL: THE *BONA FIDE* PURPOSE RULE

Hypothetical No. 2: *R. v. Saikaley*

- The RCMP e-mail
- The “Lookout”
- The ring/invoice



REGULATORY → CRIMINAL: THE *BONA FIDE* PURPOSE RULE

Special Applications:

(1) Dual Purpose Searches

- *R. v. Nolet*, [2010] 1 S.C.R. 851 at paras. 41, 43

(2) Parallel Investigations

- *R. v. Jarvis*, [2002] 3 S.C.R. 757 at para. 97
- *Jackson v. Vaughan*, 2010 ONCA 118 at paras. 45-46



REGULATORY → CRIMINAL: THE *CONSISTENT USE* RULE

Key Question:

- Would anyone with a residual privacy interest in the seized information maintain a reasonable expectation that, although the information at issue is now lawfully in the hands of the state, it would not be shared for the purpose underlying the recipient's investigation?



REGULATORY → CRIMINAL: THE *CONSISTENT USE* RULE

R. v. D'Amour (2002), 166 C.C.C. (3d) 477 (Ont. C.A.)

- Accused receiving social assistance
- In order to collect benefits, has to disclose financial affairs; welfare regulator compelled her to produce her T4 slips
- Those T4 slips revealed that she may have committed welfare fraud
- Information shared with police for criminal investigation



REGULATORY → CRIMINAL: THE *CONSISTENT USE* RULE

R. v. D'Amour (2002), 166 C.C.C. (3d) 477 (Ont. C.A.)

Holding:

- No section 8 violation. The accused could have no reasonable expectation that the information would not be shared for purpose of investigating welfare fraud.
- The information was shared with police for a purpose consistent with its initial gathering.



REGULATORY → CRIMINAL: THE *CONSISTENT USE* RULE

R. v. D'Amour (2002), 166 C.C.C. (3d) 477 (Ont. C.A.)

[T]he use of the [disclosed information] in the criminal prosecution for the fraudulent receipt of benefits did not amount to the use of the document for a purpose different from the enforcement of the *Act*. The prosecution for fraud, just like a prosecution under the *Act*, was aimed at preserving the integrity of a benefits program **Had the Department turned the [information] over to the police in aid of a prosecution that had nothing to do with the enforcement of the *Act*, the assessment of the appellant's privacy expectations might well have been different.**



REGULATORY → CRIMINAL: THE *CONSISTENT USE* RULE

Inconsistent Use:

If the parties propose to share for an “inconsistent purpose,” they must undertake a contextual analysis and assess whether sharing might engage a residual expectation that, although now in the hands of the state, the information at issue would not be put to the recipient’s proposed inconsistent use.



REGULATORY → CRIMINAL: THE *CONSISTENT USE* RULE

Hypothetical No. 1:

Accused tells the police that his personal safe was stolen from inside his restaurant, and he asks them to find it. The police discover the safe abandoned in an open field. They seize it and take it back to the station for further investigation – to see who stole it. Their review turns up documents located inside the safe that suggest the owner is engaged in tax fraud. They share the documents with *Canada Revenue*. Section 8 violation?



REGULATORY → CRIMINAL: THE *CONSISTENT USE* RULE

R. v. Law, [2002] 1 S.C.R. 227

Holding:

- The use and sharing of the documents violated section 8 of the *Charter*
- The accused retained a residual expectation of privacy in the contents of his safe; and
- The police authority to investigate the theft did not extend to unrelated investigations:
 - “While a reasonable accused would have expected a certain degree of state intrusion into his stolen safe – a fingerprint analysis, a security check, an investigation of content for the purpose of identifying the perpetrator of the theft – he would otherwise have expected the contents of the safe to remain private.”



REGULATORY → CRIMINAL: THE *CONSISTENT USE* RULE

Hypothetical No. 2:

Accused is receiving unemployment benefits when she goes on vacation. Upon return, she fills out a customs card and discloses information that calls into question her entitlement to the benefits. *Canada Customs* shares the information with the *Unemployment Insurance Commission* pursuant to a formal written agreement to share such information. The Commission prosecutes her for violating unemployment laws. Section 8 violation?



CRIMINAL → CRIMINAL: GENERAL PRINCIPLES

Same two rules apply

- (1) Bona fide purpose
- (2) Consistent use

Wakeling v. United States, [2014] 3 S.C.R. 549

Law enforcement officials have a common law authority to share lawfully seized information with other law enforcement officials (both domestic and foreign) so long as they do so for a valid law enforcement purpose.

At least in the case of sharing private communications, section 8 of the *Charter* is not extinguished by the original seizure – there is a residual expectation of privacy that applies at the “sharing” stage



INFORMATION SHARING AGREEMENTS

- As a general rule, those sharing information should do so pursuant to a written agreement.
- Purpose:
 - (1) Clear record of information shared
 - (2) Identify the terms of sharing
 - Who may use information
 - What information is being shared
 - Purpose of disclosure
 - Terms and conditions for use
 - Confidentiality and retention
 - Sunset and termination



CROWN PERSPECTIVE ON SHARING OF INFORMATION BY STATE AGENTS

- Whether we use it domestically or not, there is nothing wrong with sharing evidence of your criminal activity with any other criminal law agency (foreign or domestic)

DEFENCE PERSPECTIVE ON SHARING OF INFORMATION

- “Oh no you didn’t.” When you shared the information you deprived me of my ability to challenge the lawfulness of the original seizure



NON STATE AGENTS → STATE AGENTS

- *What happens when a private company or record holder decides to share “private” information with state agents in the absence of a state request – does s.8 apply?*
- *R. v. Spencer is not really an answer – police requested information*
- *Modern world of corporate responsibility*
- *Microsoft, Facebook, Google deciding to provide information to state agents about alleged criminality (child pornography, money laundering, terrorism, etc.)*