IAC-06-E.6.3.12

57th International Astronautical Congress 2006

DRAFTING LEGISLATION TO REGULATE COMMERCIAL REMOTE SENSING SATELLITES: A HOW-TO GUIDE FROM CANADA

Mr. Bruce Mann
Government of Canada
(Canada)
bruce.mann@international.gc.ca

Abstract

When the Canadian Space Agency (CSA) and MacDonald, Dettwiler and Associates Ltd. (MDA) proposed a jointly funded, but commercially operated RADARSAT-2 remote sensing satellite, the Government of Canada announced that it would regulate commercial remote sensing systems operated from Canada, in order to address Canadian security, defence and foreign policy issues that were bound to arise with increasingly higher performance satellites. The announcement included a 20 point *Canadian Access Control Policy* that, among other things, reserved the government's right to review and approve satellite systems, invoke shutter control over any satellite, and obtain priority access to satellite data.

A year later, the June 16, 2000 *Agreement Between the Government of Canada and the Government of the United States of America Concerning the Operation of Remote Sensing Satellite Systems*, referring specifically to the RARARSAT-2 project, called on Canada to enact the *Access Control Policy* into law, and at the same time ensure that Canadian commercial satellites would be controlled in a "comparable manner" to United States systems. The lawyers in the Department of Justice knew that a challenging legislative drafting task lay ahead of them.

Canada's *Remote Sensing Space Systems Act* is examined from the perspective of its drafters, explaining why it is written as it is. The *Act* reflects concerns about national security, defence, environmental protection, public safety and foreign policy interests, including the desirability of sensed states being able to obtain data about their own territory as set out in the U.N. *Principles Relating to Remote Sensing of the Earth from Outer Space*. The final product, which became law on November 25, 2005, meets Canada's needs by incorporating all aspects of the *Canadian Access Control Policy*, and at the same time meeting the comparability commitment in the *Canada-US Agreement*. This latter consideration is very important to the success of RADARSAT-2 because of the high degree of international cooperation involved, notably in obtaining US export permits for certain components of the satellite. Unexpected difficulties and pleasant surprises arising from the export control regime are described.

This paper can serve as a "how to" guide for jurists from like-minded countries contemplating the regulation of commercial remote sensing satellite systems.

Introduction

Since the launch of RADARSAT in 1995 the Canadian Space Agency (CSA) has managed the synthetic aperture radar satellite as a governmental operation. The CSA has sold data and imagery worldwide–looking very much like a commercial undertaking–without the guidance or control of any Canadian remote sensing satellite legislation.

However, shortly after the Canadian Space Agency's announcement in February 1998, that they had awarded a contract to MacDonald, Dettwiler and Associated (MDA) to construct and manage RADARSAT-2, government lawyers in Ottawa started dreaming of new laws to restrict, regulate, supervise, audit and police the Canadian remote sensing industry. Or at least that is how it must have seemed to MDA.

Canada's Remote Sensing Space Systems Act was passed by Parliament in November 2005, and will come into force soon, in anticipation of the launch of RADARSAT-2 which is scheduled for March 2007. The purpose of this paper is to explain why it was necessary to enact legislation governing the operation of commercial remote sensing satellites and why we drafted the Canadian legislation as we did. Particular attention will be given to issues which

generated a great deal of discussion during the Parliamentary process: the right of sensed states to obtain data about their own territory, and the government's right of shutter control and priority access to satellite services.

The Act is available from the web site of the Department of Justice, Canada, under the heading "Laws."

Canada's interest in regulating commercial satellites

Five factors of a national character were instrumental in the Government of Canada's decision to enact legislation regulating the operation of commercial remote sensing satellite systems:

–national security, –the defence of Canada, –the safety of Canadian Forces, –Canada's conduct of international relations and –Canada's international obligations.

There was no real debate that remote sensing satellite legislation, with its underpinnings in international affairs, national security, and international commerce, was constitutionally a matter within the jurisdiction of Canada's federal Parliament to legislate, even though satellite control in theory could be carried out entirely within or from a single province of Canada.

Three other factors, for which the Government of Canada has responsibility at a national level, were also involved in the decision to legislate:

–the environment, –public health and –the safety of persons and property.

All of these factors are recited throughout the Act as matters to guide the government in the issuing of licences and the regulation of remote sensing satellite systems.

Another fundamental driver of Canadian legislation was the issue of liability for damage caused by Canadian space activity, even when carried out by non-governmental entities. Under the United Nations Outer Space Treaty and the Liability Convention, Canada is liable to other states or persons in other states for injury or loss caused by satellites if the launch was carried out in Canada, or was procured elsewhere by Canada or by a Canadian person. As a matter of risk management, it is up to Canada to regulate its own nationals and any other persons whose activities could incur liability on the part of Canada.

Canada–United States Treaty sets parameters for legislation

International Treaties do not have the force of domestic law within Canada. It is necessary for Canada to enact legislation implementing such treaties. The June 16, 2000 Agreement between the Government of Canada and the Government of the United States of America concerning the Operation of Commercial remote Sensing Satellite Systems was signed with the RADARSAT-2 satellite in mind, and in fact referred to the satellite in the text. A very clear expectation was established in the Agreement that legislation would be put in place, and that it would follow certain lines as set out in the first three clauses of the Agreement:

"1. The parties agree to ensure that such commercial remote sensing satellite systems will be controlled by each Part in a comparable manner in order to protect and serve shared national security and foreign policy interests".

This clause committed Canada to enacting legislation similar in principle to the United States Land remote Sensing Policy Act and related rules including the capability for the government to obtain exclusive access to satellite services in critical situations.

"2. Canada agrees to keep in place, until its provisions are enacted into law, the Canadian national access control policy announced on 9 June 1999, set forth in Annex I hereto, concerning such commercial remote sensing satellite systems owned, operated or registered in Canada".

The access control policy, which had been developed by a Canadian government interdepartmental team, was the cornerstone for the government's drafting instructions for the Remote Sensing Space Systems Act. It included the most fundamental and controversial elements of the legislation that followed:

–Canada's right to review and set limits on data access, system architecture, system performance and foreign ownership of remote sensing satellite systems.

–Shutter control—the interruption of normal commercial service where the availability of data could be detrimental to Canada's national security and

foreign affairs interests.

–Priority access where data would be beneficial to national security and foreign affairs interests.

The access control policy also listed 17 obligations on the satellite operator ranging from the requirement to maintain positive control of the satellite from Canada at all times to the requirement to make data available to sensed states in accordance with the United Nations Principles Related to Remote Sensing of the Earth from Space. Obligation 4, "Obtain export or import permits(s) pursuant to applicable to laws" presumably was included because four critical modules in RADARSAT-2 incorporate technology for which an export permit was required under the United States International Trafficking in Arms Regulations (ITAR), even though the launch was expected to be from Vandenberg, California. An export permit was required for the assembly of the spacecraft in Europe and Canada.

We incorporated all the elements of the policy in the legislation, (except for item 4, which did not require legislation) substantively or in the form of enabling provisions giving the government the authority to enact regulations.

Although the ITAR requirement for United States export permits was not mentioned in the Canadian legislation, it had a significant impact on the RADARSAT program. Without going into details, employees of the CSA were scrutinized as to their place of birth, and other citizenship in the case of dual nationals. Under ITAR policy rules, contact with or exposure of sensitive technology requiring an export permit to a person who is a national of a proscribed country constitutes a "deemed export" of the technology to the proscribed country. As a result, the CSA was required to keep certain employees away from sensitive technology or meetings where technology was discussed, on the basis of their place of birth, even if the employees were Canadian citizens with high level security clearances.

Ironically, the ITAR rules facilitated the RADARSAT-2 launch plans in 2005 when, for technical reasons, it became necessary to use a Soyuz launch vehicle from Baikonur, Kazakhstan. A tripartite agreement exists between the United States, Russia and Kazakhstan, which enables the launch of United States spacecraft from Baikonur under the supervision of United States Defense Technology Security Administration (DTSA) personnel, and exempts spacecraft from customs inspections in Russia and Kazakhstan. Because RADARSAT-2 contains technology requiring United States export permits, RADARSAT-2 qualifies as a United States Spacecraft under the Baikonur launch agreement, and can be launched without Canada having to negotiate a separate agreement with Russia and Kazakhstan.

3. Canada agrees to implement controls pursuant to this Agreement, set forth in Annex II hereto, which is protected as commercially confidential, with regard to the operator of RADARSAT-2.

This clause in the Agreement obliges Canada to put in place restrictions on performance characteristics of the satellite and the remote sensing space system, ultimately resulting in limits to the resolution of imagery from satellite data. The House of Commons Standing Committee on Foreign Affairs and International Trade examined Annex II in camera to confirm that it did indeed contain only technical parameters, and not secret priority access rights in favour of the United States as suggested by one Committee witness.

Performance limits are not part of the legislation, but the legislation does specifically authorize the Minister of Foreign Affairs to set conditions for a licence which will include approved performance limits. This information is considered commercial confidential because its disclosure could give an unfair advantage to competitors from other jurisdictions if they knew the actual performance limits of RADARSAT-2 or the limits that the Government of Canada intends to impose. Presumably the satellite operator will seek amendment of the performance limits as international competitors offer higher resolution imagery and it becomes pointless for Canada to maintain more stringent restrictions for security purposes.

Act applies to public and private sector

Section 4 of the Act states "This Act binds Her Majesty in right of Canada or a province," formal Canadian statutory language directing that government departments and agencies at all levels in Canada are subject to the legislation. Even the Canadian Space Agency, which has operated the

original RADARSAT satellite for eleven years, will be subject to the licensing regime of the Act.

The reason we used this approach in the legislation was because of the difficulty and uncertainty in attempting to confine the application of the legislation to commercial satellites. What did we mean by commercial? Does the term imply non-governmental, for-profit ownership of the satellite? Or is the nature of the use of the satellite the appropriate criterion? RADARSAT-2, destined to be the first satellite to be licensed in Canada, has been described all along as a commercial satellite, but the fact that it is more than 75

This definition is broad in scope and includes satellites with optical, thermal infra-red, and other types of sensors–not just synthetic aperture radar satellites such as RADARSAT and RADARSAT-2. Even weather satellites come within the purview of the Act. However, individual satellites, or classes of satellites, or specific uses of satellites can be exempted from the licensing requirement of the Act, as will be discussed later.

Act applies to operations carried on outside Canada

Persons carrying on remote sensing space system activities (including satellite control, and data gathering, treatment and delivery) within Canada or from Canada, of course are subject to the Act—just as they are to other Canadian legislation. To protect Canada's national interests, and risk manage potential liability, the requirement for a Canadian satellite licence also applies to the following categories of persons in respect of their activities outside Canada:

(a) Canadian citizens;

(b) Permanent residents. These are people who have legal status entitling them to remain in Canada and generally enjoy most of the rights and responsibilities of Canadian citizens;

(c) Canadian corporations. This includes companies with a Canadian charter, i.e. actually incorporated in Canada, as well as companies that have converted their corporate citizenship from another country to federal or provincial jurisdiction within Canada;

(d) Specified persons tied to Canada. The federal government can enact regulations defining classes of persons (individuals, corporations, partnerships, etc.) who have a connection to Canada related to remote sensing space systems that warrants bringing them within the ambit of the legislation. An example might be foreign persons who procure the launch of a satellite from Canada. We made this provision open-ended so that the government could deal relatively quickly with unexpected situations. Federal regulations can be enacted in an abbreviated time frame, if necessary. Unlike statutes, they are not dependant on Parliament being in session.

Exemptions from the Act

The foregoing broad-reaching provisions were drafted ex abundante cautela. We considered this necessary to promote Canada's national interests to the maximum extent possible, and to protect Canada from liability. To avoid inappropriate application of the Act, the Minister of Foreign Affairs is authorized to exempt any persons, satellite systems, or data, on an individual or class basis, from any or all aspects of the licensing regime, so long as the Minister is satisfied that none of Canada's national interests will be compromised. For example, if Canadians are involved in the operation of a satellite system licensed by a foreign country, it would be appropriate to clarify by Ministerial order that the system is exempt from the Act, or at least is exempt insofar as those Canadians are concerned.

Where the Department of National Defence or the Canadian Space Agency operates a remote sensing satellite system, the government may issue a Cabinet order modifying or adapting any provisions of the Act for that application. We drafted this provision as a compromise, instead of completely exempting either of these federal government entities from the Act. This will ensure that any commercial operations carried out by either entity (most notably the CSA) will remain subject to the same international data distribution controls set by the Minister of Foreign Affairs for normal commercial operators. Yet for their own governmental or military uses of remote sensing satellites, they can be exempt from the Act. To further maintain their independence from the Minister of Foreign Affairs, neither National Defence nor the CSA have to apply to Foreign Affairs for an exemption order. The special order modifying or adapting the Act for their purposes is issued by the federal Cabinet.

It is anticipated that as soon as the remote sensing

legislation comes into force, an order will be issued either by the Minister of Foreign Affairs or the federal Cabinet exempting the CSA from any licensing requirements for the original RADARSAT satellite.

Time limits and representations

A criticism that was raised on several occasions during and after the legislative process is that the Act does not contain time limits, such as the time within which the Minister of Foreign Affairs should issue a licence after an application is filed.

A satellite licence is extremely complex. The application process involves the submission and consideration of information ranging from technical details of the proposed satellite system and its capabilities, to financial and other corporate information about the licensee and potential system participants, and details of prospective sales agreements. Establishing customer access profiles (CAPs), an intricate series of conditions for the distribution of data and remote sensing products, involves considerable dialogue about who is to receive data, about which sensed territories, at what resolution, and after what time delay. Throughout the application process the applicant will have the opportunity to make representations about all aspects of the requested licence. It did not make sense to set a time limit for the complex, variable application process.

Because of the interactive nature of the application process, we did not provide in the Act the right to make representations after a licence application is refused. However, in order to give a rejected applicant the opportunity to challenge a refusal to grant a licence, the Minister is required to provide reasons to the applicant for the refusal, which can be made the subject of judicial review.

Another feature in the legislation designed to relieve some of the time pressure in an initial licence application is the authority to grant a provisional approval of a licence application, which is binding on the Minister of Foreign Affairs so long as the material facts on which the approval was based remain substantially unchanged. This provision in the legislation was inspired by a request from MDA for the Minister of Foreign Affairs to issue a latter approving the terms of a contract that MDA was negotiating with a data customer for RADARSAT-2 services.

The only time limit binding on the government is when a satellite licence is suspended. The Minister of Foreign Affairs must decide within 90 days whether the licence is to be cancelled, otherwise the suspension will end and the licence is restored. In other situations, such as an application for a licence or for a change in licence conditions, with national security issues at play, it would not make sense to issue a license by default if the government failed to reach a decision within a time limit.

This being said, the Act authorizes the government to make regulations respecting the issuance, amendment and renewal of licences, which could include time limits for the government to respond. Alternatively, the Minister has authority to establish policies and guidelines which could include time frames for government action. Under Canadian law, if government action is not forthcoming, an affected person has recourse to the Federal Court of Canada for prerogative relief in the nature of mandamus, compelling the relevant government official to do his or her job.

Mandatory licence conditions

Although the Minister of Foreign Affairs can set out conditions of any kind in a licence, mandatory conditions were included in paragraphs 8(4)(a) to (g) of the Act to inform satellite operators and data customers of certain fundamental obligations:

(a) The licensee must keep control of the system. This refers to functional control by the person who operates the system. There are a number of exceptions, perhaps better referred to as clarifications, elsewhere in the Act which permit others to control a satellite of a system, so long as the licensee maintains overriding control. Also, the Minister may specifically approve someone else taking control of a satellite, or approve a complete transfer of the licence to someone else.

(b) It is up to the licensee to ensure that only persons specifically authorized in the licence perform certain controlled activities. In the normal operation of a remote sensing space system, the Act does not call on the government to directly regulate the activities of anyone but the licensee.

(c) This mandatory licence condition derives from Principle XII of United Nations Resolution 41/65, adopted on December 3, 1986, Principles Relating to Remote Sensing of the Earth from Outer Space, which gives sensed states access to certain data con-

cerning their territory.

Principle XII

As soon as the primary data and the processed data concerning the territory under its jurisdiction are produced, the sensed State shall have access to them on a non-discriminatory basis and on reasonable cost terms. The sensed State shall also have access to the available analysed information concerning the territory under its jurisdiction in the possession of any State participating in remote sensing activities on the same basis and terms, taking particularly into account the needs and interests of the developing countries.

The sensed state's right is expressed in the legislation in terms of a mandatory licence condition obliging the licensee to make raw data and remote sensing products available to the government of the sensed state. This right of access in not unrestricted, as limitations on the rights of sensed states are inherent in the definition of "remote sensing" used by the UN:

Principle I

For the purposes of these principles with respect to remote sensing activities:

(a) The term "remote sensing" means the sensing of the Earth's surface from space by making use of the properties of electromagnetic waves emitted, reflected or diffracted by the sensed objects, for the purpose of improving natural resources management, land use and the protection of the environment. [emphasis supplied]

There is no obligation to provide sensed states with data for purposes other than improving natural resources management, land use, and protection of the environment. In practical terms, this means that sensed states will not automatically be entitled to receive sensitive, high quality information gathered by sensing states for security purposes or which raises security concerns. Customer access profiles established and maintained by the Minister pursuant to the licence, along with other licence conditions, may limit the nature and timeliness of information that the licensee is required to provide to sensed states.

This interpretation of the UN principles is certainly subject to debate. Some would argue that the sensed state's right of access need not be mentioned at all, since the UN resolution is not binding, and probably never will be. Nevertheless, the Parliament of Canada approved paragraph 8(4)(c) of the Act based on the foregoing interpretation of the UN principles.

The underlying theme of UN Principle XII, as it has been incorporated in paragraph 8(4)(c) of the Act, is to prevent discrimination against the government of a sensed state as a purchaser of raw data or remote sensing products from the licensee for management of natural resources, land use and protection of the environment. For example, the licensee cannot provide such data or products to someone else on an exclusive basis, nor can it restrict access to such information about the sensed state to the highest bidder. The licensee is obliged to offer the raw data or remote sensing products (subject to the limitations discussed above) in a timely manner at reasonable rates. This obligation does not extend to enhanced data or value-added products, which the licensee may sell on a competitive basis to whomever the licensee chooses.

The licensee is not obliged to store data indefinitely for the possible use by the sensed state. The obligation to provide data or remote sensing products exists only so long as they have not been disposed of.

(d) The condition requiring the licensee to keep control of raw data and remote sensing products until they are disposed of has two facets to it. The "sale" of data to customers cannot be an outright transfer of all proprietary rights to the customer. It is standard industry practice to maintain such control by entering into system participant agreements and end-user licence without conveying intellectual property rights associated with the data. The other facet to condition (d) is the requirement to honour the terms of the system disposal plan (see section 9), which will spell out the circumstances in which the licensee may dispose of data and products. The plan could call for the destruction of data, the government's right to acquire all interests in the data or the right to convey all interests in data to other persons approved by the Minister.

(e) The condition that raw data from the system may be communicated only to authorized persons is fundamental to the security of the system. Normally raw data will be communicated only to system participants, since the communication of

raw data is a controlled activity, but this provision recognizes that there can be exceptions–where the government of a sensed state is entitled to receive raw data in accordance with condition (c) discussed above, or where the Minister, in the licence, expressly authorizes such communication to other persons.

(f) This condition is somewhat unusual. Under paragraphs 8(6)(b) and 8(7)(b) of the Act the Minister of Foreign Affairs can require that the communication of raw data or remote sensing products be done under a legally enforceable agreement respecting their security and non-disclosure. It is up to the licensee to police the agreement and "encourage" system participants and other persons who receive data to handle it appropriately. This encouragement could be accomplished through legal action for breach of the agreement or other means, such as cutting off the supply of data or products to customers who do not comply. The Minister, in turn, can require the licensee to enforce the agreement by means of administrative monetary penalties, by suspending the licence, or by taking other more serious corrective measures if the licensee violates this condition.

(g) Paying fees has been set as a condition of a licence so that failure to pay can be dealt with as a breach of condition.

Conditions set by the Minister

Two kinds of conditions that are almost certain to be set are described in subsection 8(5): conditions relating to cryptography and information assurance; and conditions naming system participants and the controlled activities the licensees may allow them to perform.

Customer access profiles (CAPs) are authorized by this clause, as well as by clauses 8(6) and 8(7) which follow. CAPs are detailed sets of conditions on the dissemination of raw data and remote sensing products, including rules for the communication of raw data and remote sensing products among the licensee, system participants and their customers. They very likely will include a proscribed entity list, naming entities that are prohibited from receiving raw data or remote sensing products under various circumstances.

Shutter control

By analogy to restrictions on time and place of exposures taken by a conventional camera, orders for the interruption or restriction of land sensing operations of a remote sensing satellite are popularly called "shutter control" orders. In the context of a synthetic aperture radar satellite, such as RADARSAT 2, a shutter control order could entail any combination of a complete cessation of sensing activities over certain territories or at certain times, attenuated sensing performance, delays in downloading data from the satellite, restrictions on the resolution of remote sensing products, and delays or outright bans on the provision of certain data products.

No one objected to the concept of shutter control, accepting the premise that for matters of national security, the state must be able to prevent the collection of data inimical to national interests. Complex criteria for the exercise of shutter control could delay or prevent its implementation, and for this reason were rejected. Instead, three safeguards against the misuse of shutter control were adopted: (1) An order can be made only by the Minister of Foreign Affairs or the Minister of National Defence. No delegation of authority is permitted. (2) A potential injury test, appropriate for each Minister's portfolio, must be met for the Minister to make a shutter control order. (3) The licensee has the opportunity, after the fact, to make representations about the order, which may be helpful to the licensee to persuade the Minister that other measures can be taken in lieu of continuing or repeating shutter control.

Up to date fine tuning of the Customer Access Profiles (licence conditions setting out the parameters for distribution of data about sensed territories) will reduce or eliminate the need to invoke shutter control. The experience in the United States has been that despite having exclusive access authority for over 20 years, the government has never had to use its shutter control power over commercial satellites.

Priority Access Priority access refers to the government's right to jump the queue for the provision of services from a remote sensing space system in urgent circumstances.

The tests that the Minister of Foreign Affairs, the Minister of National Defence, or the Minister of Public Safety must meet in order to justify a prior-

ity access order are geared to their respective portfolios, on the grounds that they are desirable for the listed purposes. For this reason academics, industry officials and Parliamentarians all expressed concern during Committee hearings about abuse of this exceptional power, to the detriment of remote sensing satellite operators who would not only lose revenue from displaced customer service, but would not be compensated by the government for the expropriation of services. The fact that the government is immune to claims for damages resulting from shutter control orders or priority access orders only heightened this concern.

Ultimately, Parliament was satisfied that mitigating factors in the Act minimized potential loss to operators, and enacted these elements of the legislation without amendment. The mitigating factors were as follows:

Ministers can delegate the power to issue priority access orders only to their respective deputy ministers or certain agency heads, namely, the Chief of the Defence Staff, the Commissioner of the Royal Canadian Mounted Police (RCMP - Canada's federal police force) or the Director of the Canadian Security Intelligence Service. No further delegation is permitted. RCMP orders are confined to the investigation of offences arising from threats to the security of Canada. The RCMP cannot use priority access orders for their other domestic policing responsibilities.

The licensee has the opportunity, after the fact, to make representations about the order. This may assist the licensee in working out a level of priority for the order that will meet the relevant Minister's requirements while minimizing the interference with other commercial business. It is anticipated that government needs, even on an urgent basis, will be met through the licensee's commercial priority service ordering process and, as in the United States, a statutory order for priority access will never be necessary.

No liability for government intervention

The "No Liability" provision in the Act gives the government immunity from claims for financial losses for actions taken in good faith, but does not prevent the government from providing compensation on a voluntary basis, under normal ex gratia prerogative authority. In the case of priority access orders, the Act specifically authorizes the Minister who made the order to pay the satellite system licensee an amount determined in accordance with government regulations for the service. Draft regulations have been prepared and discussed with MDA, which will ensure that satellite operators receive the same level of compensation they have received over the previous year for commercial services on a priority basis, or an otherwise agreed upon level of compensation.

The single greatest advocacy task for the Department of Justice in the course of development of the Act was to convince sceptics that the permissive language of the Act ("A Minister may pay a licensee an amount determined in accordance with the regulations...") did not give the Minister an unfettered discretion to refuse to pay compensation. There is ample jurisprudence in Canada to the effect that such permissive language in a statute actually creates an obligation to act where all the required conditions for action have been met.

Powers of Inspection and Audit

The powers of inspectors in the Remote Sensing Space Systems Act are typical of those found in other Canadian statutes, and respect the right to be secure from unreasonable search and seizure under the Canadian Charter of Rights and Freedoms. For example, a judicial warrant is required before an inspector can enter a private dwelling without the consent of the occupant.

While the Act specifically claims jurisdiction over Canadians and certain other classes of persons outside of Canada in respect of the prohibition on operating a remote sensing space system without a licence, no extra-territorial claim is made about the powers of inspectors outside Canada.

This does not necessarily mean that inspectors are prohibited from entering the premises of system participants and other persons in foreign jurisdictions. The authorities in other countries may be prepared to allow, or even assist, inspectors to enter premises in their jurisdiction under mutual legal assistance agreements between Canada and foreign countries. Also, a licensee may enter into agreements with system participants or end users in foreign jurisdictions in which those persons specifically agree to let the licensee, or persons designated by the licensee (including Canadian government in-

spectors), enter their premises to conduct inspections and perform audits.

Rather than require inspectors to cart away boxes of documents, tapes and data storage devices, which could harm the affected person's capacity to carry on business, the Act gives inspectors the slightly more intrusive, but less disruptive, powers to examine things on site, test equipment, use equipment to generate records, and make copies of records to take away for examination.

Both the obligation to assist inspectors and the prohibition against obstructing inspectors or providing false information to them are offences under the Act. We are doubtful that someone could be prosecuted in Canada for an obstruction that took place outside Canada. However, it is possible that the offence of providing false information could be prosecuted in Canada if it could be shown that the person in question knew and intended that the false information would be taken back to Canada by the inspector.

These questions are largely academic because the enforcement of the Act weighs mainly on the licensee, with the expectation that the licensee will facilitate investigations and provide information as requested.

Requests for Information

For the most part, monitoring compliance with the Act will be a matter of reviewing records of data collection, treatment and transmission. The Minister can request any person to provide pertinent information or documents. There is no reason to expect non-compliance, but if a request is refused or ignored it can be the basis for an order by a superior court or the Federal Court of Canada for an order requiring production of the information or documents. A judge may order a person to produce information or documents if satisfied that they are necessary under the regulatory scheme, and the public interest in having the information or documents outweighs other interests, including the person's right to privacy.

The advantage of a judicial order is that it can be enforced through the court system by means of access to the person's premises and the possibility of penal sanctions for contempt of court.

Foreign countries may not be willing to enforce a Canadian Minister's request for information or to give Canadian inspectors the right to operate in their jurisdiction. However, at the judicial level, most courts of superior jurisdiction in the world honour the custom of letters rogatory, or mutual legal assistance conventions, under which they will exercise their own inherent jurisdiction to compel persons within their territory to appear, produce documents, and answer questions, at the request of a judge in another jurisdiction.

Administrative Monetary Penalties

Except for a few very serious contraventions of the Act, for which heavy fines and prison sentences may be imposed, the Act regulates conduct through administrative monetary penalties (AMPs) for violations, with the option of entering into voluntary compliance agreements and terminating the violation proceedings. The emphasis is on correcting conduct at the earliest possible opportunity.

For the most part the violation provisions are directed at licensees, including employees of licensees, for breaches of licence conditions. Licensees are expected to make sure that their system participants and customers follow the rules.

Violation proceedings begin with the issuing of a notice of violation. The recipient may pay the fine set out in the notice, ending the matter. Alternatively, the person may exercise the right to make representations about the violation to the enforcement officer, who will decide whether the person committed the violation. During the course of the representations, the enforcement officer may enter into a compliance agreement with the person, ending the proceedings without a violation record–so long as the person abides by the compliance agreement.

If a penalty is imposed, the person has the right of appeal to the Minister. As with any Ministerial decision, the Minister's disposition of the appeal is subject to judicial review.

We considered another novel system where licensees would be immune from prosecution for violations that they identified, admitted, and corrected before being detected by regulators. However, we did not consider this appropriate in an environment where the regulator learns of improprieties so long after the fact. Such a system might lead licensees to deliberately flout the rules and

capitalize on data sales, with the knowledge that they could admit to and correct their misconduct before government auditors would notice it. The AMPs system strikes an appropriate balance between self-regulation and liability for misconduct.

Consistent with the principle of adjusting conduct at the earliest opportunity, rather than penalizing parties for breach after the fact, the Act contains a special injunction authority, enabling the Minister, with the assistance of a Court, to take steps to prevent someone from operating a remote sensing space system unlawfully. The proposed or purported transfer of ownership of a remote sensing satellite system, without having notified the Minister, could be grounds for an injunction against the licensee or former licensee, or the person intending to acquire the system, blocking the transfer.

The injunction power is the only way to deal with persons who are not, and never have been, licensees, before they commence an unlawful operation.. The Court can order them to take any measure that a licensee could be ordered to take under the Act.