FIRST LICENCE ISSUED UNDER CANADA'S REMOTE SENSING SATELLITE LEGISLATION

Bruce W. Mann[*]

BACKGROUND

Since the launch of the first *RADARSAT* satellite in 1995, the Canadian Space Agency (CSA) has been responsible for the collection, processing, and delivery of its synthetic aperture radar (SAR) satellite imagery worldwide, including sales and distribution through private sector partners.

However, when CSA announced in February 1998, that they had awarded a contract to MacDonald, Dettwiler and Associates (MDA) to construct, own and manage a new, more powerful SAR satellite, *RADARSAT-2*, it became apparent that regulation of the commercial satellite operator would be required to protect Canada's national security and international affairs interests, as well as public interests in the environment and safety of persons and property.

On June 16, 2000 the Agreement between the Government of Canada and the Government of the United States of America concerning the Operation of Commercial Remote Sensing Satellite Systems[1] (2000 Canada-US IGA) was signed, facilitating the export of United States technology, with the *RADARSAT-2* satellite specifically in mind. A very clear expectation was established in the first clause of the Agreement about the nature of legislation that would be enacted in Canada:

> The parties agree to ensure that such commercial remote sensing satellite systems will be controlled by each Party in a com-

---

[*] Barrister & Solicitor, Department of Justice, Ottawa, Ontario, Canada.

[1] Agreement between the Government of Canada and the Government of the United States of America concerning the Operation of Commercial Remote Sensing Satellite Systems, U.S.-Can., June 16, 2000, 2000 Can. T.S. No. 2000/14 [hereinafter 2000 Canada-US IGA].

> parable manner in order to protect and serve shared national security and foreign policy interests.[2]

Canada's Remote Sensing Space Systems Act[3] (Act), and Remote Sensing Space Systems Regulations[4] (the Regulations) implement a licence and control regime comparable to the United States Land Remote Sensing Policy Act and related licensing rules.[5] The legislation places 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.[6] This paper builds on and complements other works[7] tracing the development of Canada's Access Control Policy for remote sensing satellite data through to the issuance of the first satellite licence to MDA Geospatial Services Inc on November 15, 2007. The *RADARSAT-2* satellite was successfully launched on December 14, 2007.

---

[2] *Id*.

[3] *See* Remote Sensing Space Systems Act, 2005 S.C., ch. 45 (Can.).

[4] *See* Remote Sensing Space Systems Regulations, SOR/2007-66 (Can.).

[5] *See* Land Remote Sensing Policy Act of 1992, 15 U.S.C., ch. 82 (1992*). See also* Licensing of Private Land Remote-Sensing Space Systems*,* 15 C.F.R. § 960 (2006).

[6] Principles Relating to Remote Sensing of the Earth from Outer Space, United Nations Resolution 41/65, adopted on December 3, 1986 [hereinafter Principles Relating to Remote Sensing].

[7] Phillip Baines outlines the development of Canada's Access Control Policy from 1995 to 2003 for satellite data in Phillip Baines, *Balancing Interests: Toward further progress in the development of a regulatory regime for commercial remote sensing space systems in Canada*, *in* PROCEEDINGS, THE FIRST INTERNATIONAL CONFERENCE ON THE STATE OF REMOTE SENSING LAW (Joanne Gabrynowicz, ed., The National Remote Sensing and Space Law Center, 2002) Bruce Mann joined Mr. Baines in 2003 to put Canada's Access Control Policy into law, and reports on work to 2006, from the perspective of a legal practitioner in, Bruce Mann, *Drafting Legislation to Regulate Commercial Remote Sensing Satellites: A How-to Guide from Canada*, *in* IISL/IAC-06 E6.3.12 (2006) [hereinafter *Drafting Legislation*]. *See* Thomas Gillon, *Regulating Remote Sensing Space Systems in Canada – New Legislation for a New Era,*34 J. SPACE L. 19 (reviews the evolution of Canada's Access Control Policy for remote sensing satellite data from its genesis in 1998 to the coming into force of Canada's legislation in 2007).

WHY REGULATE?

Canada's National Interest in Regulating Remote Sensing Satellites

With the prospect of non-governmental entities in Canada launching satellites capable of collecting sensitive data about Canada and other territories, and selling it abroad, five factors of a national character were instrumental in the Government of Canada's decision to enact legislation regulating the operation of 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.

These factors are referred to as Canada's "national interests" in this paper.

Three other "public interest" factors, for which the Government of Canada at the national level has a shared responsibility with the provincial governments, also appear in the Act:

–the environment,

–public health, and

–the safety of persons and property.

All of the above factors are recited throughout the Remote Sensing Space Systems Act as matters to guide the government in the issuing of licences and the regulation of remote sensing satellite systems.

Liability

At both the national and international level, a fundamental driver of Canadian legislation was the issue of Canada's liability for damage caused by Canadian space activity, even when car-

ried out by non-governmental entities. Under the United Nations Outer Space Treaty[8] and the Liability Convention,[9] 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.

Although the focus of the Act is the security of remote sensing data, Canada has remained sensitive to the physical risk presented by uncontrolled de-orbiting of satellites following the January 1978 re-entry of the Soviet *Cosmos 954* satellite, which spread radioactive material across Northwest Canada.

The importance of being able to bring the entire satellite back to Earth at mission end was highlighted by China's controversial test of a medium-range ballistic anti-satellite (ASAT) weapon to destroy a defunct weather satellite in January 2007. The explosion of the weather satellite created an orbiting debris cloud, increasing the risk of collision with another satellite at a comparable altitude by a factor of thousands—although the level of risk still remains extremely low. The real danger is that pieces of orbital debris, some so small that they cannot be tracked and avoided, are capable of disabling another satellite, leading to the possibility of chain reaction collisions that could eventually create multiple rings of debris, rendering the low earth orbit (LEO) region of 200 – 1000 km altitude virtually unusable for a lengthy period of time, and greatly increasing the risk to spacecraft passing through the LEO region to geosynchronous orbits or other space missions.

With the foregoing risks in mind, a detailed System Disposal Plan must be submitted and approved with an application for a licence under Canada's Remote Sensing Space Systems

---

[8] *See* Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, arts. VI-VII, Oct. 10, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205.

[9] *See* The Convention on International Liability for Damage Caused by Space Objects, arts. II, VIII, Sept. 1, 1972, 24 U.S.T. 2389, 961 U.N.T.S. 187, which set out Canada's liability to other states or persons for damage caused by Canadian commercial satellite operators.

Act. A satellite licence typically will include a requirement that a satellite maintain sufficient on-board propellant to de-orbit the satellite in a controlled manner at mission end.[10]

In addition to a System Disposal Plan, Canadian licence applicants must propose arrangements to guarantee the performance of their obligations under the Plan. If approved, the arrangements become conditions of the operating licence.

SCOPE OF APPLICATION

Law Governs Anyone in Canada and Canadians Abroad

Carrying on remote sensing space system activities, including satellite control, data collection, data treatment, and data transmission, within or from Canada, is unlawful unless done under the authority of a Canadian remote sensing space system licence.[11] The requirement for a licence also applies to certain persons in respect of their activities *outside* Canada, namely: (a) Canadian citizens, (b) Permanent residents (these are people who have legal status entitling them to remain in Canada, somewhat similar to Green Card holders in the United States), (c) Canadian corporations, and (d) classes of persons as may be specified in the Regulations.

The Government of Canada 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.[12] An example might be foreign persons who procure the launch of a satellite from Canada, or who acquire a satellite from a Canadian person and intend to exercise control of the operation from outside Canada. No such regulations have been enacted yet.

---

[10] There can be exceptions. The tiny *CanX* satellite, the size of a half-gallon milk carton, to be launched by the University of Toronto in 2008, will not require positive de-orbiting so long as its orbit is low enough to bring it back to Earth in less than 25 years through natural orbital decay.

[11] Remote Sensing Space Systems Act, 2005 S.C., ch. 45, § 6 (Can.).

[12] Please cite to the source.

Law Applies to Both Public and Private Sector

In addition to private individuals and corporations, government departments and agencies at all levels in Canada are subject to the legislation.[13]

Many Types of Satellites Covered

The definition of remote sensing satellite[14] under the Act is broad in scope and includes satellites with optical, radar, thermal infra-red, multi-spectral, and other types of sensors. Even weather satellites come within the purview of the Act.

This broad approach was used in the legislation because of the difficulty and uncertainty in attempting to confine the application of the legislation to satellites that are intended for commercial remote sensing use. In fact, the term commercial is not even used in the legislation, and the intended use is irrelevant. A satellite's capability determines whether it must be licensed under the Act.

Exemptions

The far-reaching provisions of the Act were drafted *ex abundante cautela* to promote Canada's national interests and public 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[15] 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.

---

[13] *Id.* § 4. "This Act binds Her Majesty in right of Canada or a province."

[14] *Id.* § 2. Definition: "remote sensing satellite" means a satellite that is capable of sensing the surface of the Earth through the use of electromagnetic waves.

[15] *Id.* § 4(3).

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 use. 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, while strictly governmental operations can be exempt from the Act.

Effect of United States ITAR

Although the Canadian Access Control Policy in the 2000 Canada-U.S. IGA states that satellite operators will obtain import or export permits pursuant to "applicable laws,"[16] no express reference to, or obligation deriving from the United States International Traffic in Arms Regulations (ITAR)[17] appears in the Act. Nevertheless, the ITAR has had a significant impact on the *RADARSAT* programs as well as other aerospace and defence-related industries where technology has been exported from the United States to Canada under an export licence. As the United States Department of State applies the ITAR, contact with or exposure of ITAR technology to a person who is a national of a proscribed country constitutes a "deemed export" of the technology to that proscribed country. This discrimination, based on place of birth, has meant that some dual-national Canadian citizens, even though they hold high level security clearances and may have renounced their other citizenship, have not been allowed access to certain sensitive technology or meetings where technology was discussed.

Because several components of the *RADARSAT-2* satellite are ITAR-sensitive technology subject to US export licences, the operator of *RADARSAT-2*, or the exporter of the technology, could conceivably risk contravention of the ITAR if the United States Department of State concludes that there has been an unauthorized "deemed export." Canada's legislation does not

[16] 2000 Canada-U.S. IGA, *supra* note 1, at Annex I, obligation no. 4.
[17] 22 C.F.R. §§ 120-130 (2007).

incorporate the ITAR in any way, but neither does it prevent it extraterritorial application in Canada.

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 between the United States, Russia, and Kazakhstan 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 ITAR technology requiring United States export permits, *RADARSAT-2* qualified as a United States Spacecraft under the Baikonur launch agreement, and was launched without Canada having to negotiate a separate agreement with Russia and Kazakhstan.

Performance Limits

Annex II of the 2000 Canada-U.S. IGA sets out certain controls on the performance of the *RADARSAT-2* satellite that Canada agrees to implement. The actual performance limits are stated to be commercially confidential and are not published with the IGA. Specific performance limits are not set out in the Act, but the Act does authorize the Cabinet to make regulations[18] about the operation of satellite systems and the Minister of Foreign Affairs to set conditions in a licence[19] restricting the resolution, timeliness, geolocation accuracy, etc. of raw data and data products.

THE LICENCE

The first licence under the Act was issued to MDA Geospatial Systems Inc on November 15, 2007, in anticipation of the launch of *RADARSAT-2* which took place on December 14, 2007.

---

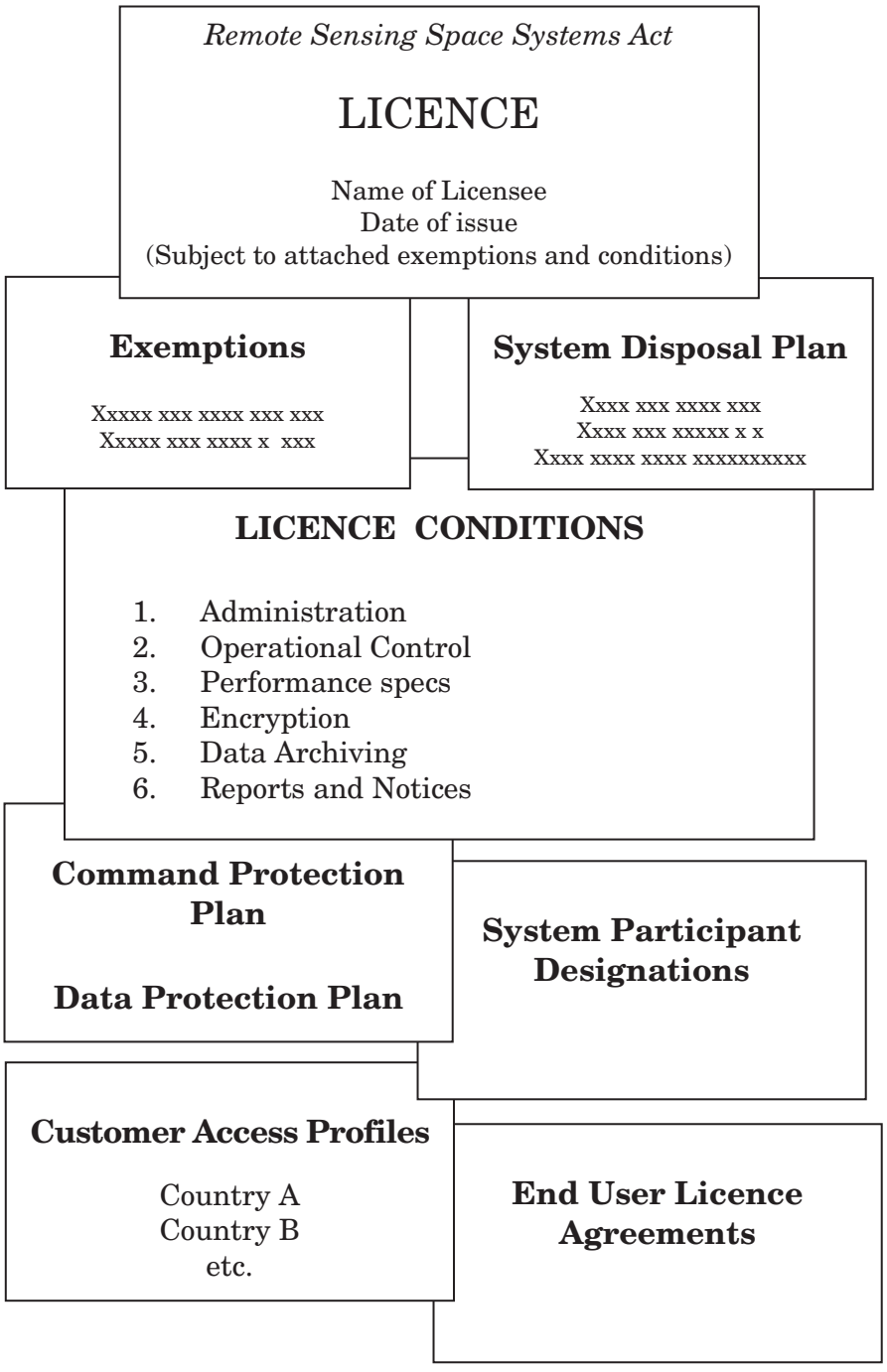
[18] Remote Sensing Space Systems Act, 2005 S.C., ch. 45, ¶ 20(1)(f) (Can.).
[19] *Id.* § 8(5)-(7).

System Disposal Plan

No licence can be issued without a system disposal plan. The Plan will vary depending on the nature of the satellite and its proposed orbit. Some mandatory elements of a Plan are set out in the Regulations, Schedule 1:

– method of satellite disposal
– amount and nature of debris expected to reach Earth
– expected location of the debris path
– space debris upon accidental or deliberate explosion
– probability of loss of human life upon satellite disposal
– disposition of satellite data.

Typical Form of Remote Sensing Space System Licence



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:

Control of the System

Paragraph (a) obliges the licensee to 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.

Controlled Activities

Paragraph (b) requires that the licensee 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.

Sensed States

Paragraph (c) is based on Principle XII of the 1986 United Nations Principles Relating to Remote Sensing of the Earth from Outer Space[20]—that sensed States should be able to obtain data about their own territory. Inherent limitations in the 20 year old principle render it largely ineffective with respect to today's technology and the heightened security concerns engendered by that technology.[21]

---

[20] Principles Relating to Remote Sensing, *supra* note 6. Principle XII deals with sensed states right to information about their territory.

[21] *See Drafting Legislation*, *supra* note 7, at pp. 6, 7 where the inherent limitations in Principle XII are discussed.

Principle XII, as incorporated in Canada's legislation, offers no advantage to non-governmental purchasers of data in a sensed state, and does not override restrictions or prohibitions on data transfer to the country in question.

The net effect of Principle XII, from Canada's standpoint, is that a Canadian satellite operator is not allowed to give *exclusive* rights to data and data products to someone in country X about the territory of country Y, and thereby prevent the government of country Y from obtaining data or data products that they otherwise would have been allowed to receive. While Principle XII may be of some value to sensed states, its real value today lies with commercial satellite operators, as it allows them to make a second sale of data that might otherwise have been sold on an exclusive basis.

Principle XII appears to be incorporated with the same effect in Germany's recent Satellite Data Security Act, which was enacted in time to regulate its new satellite, *TerraSAR-X*, launched on July 15, 2007. In fact, the German legislation may go even further by prohibiting a commercial operator from allowing a customer to prevent a third person (not just the government of a sensed state) from accessing data about a specific region.[22] In all cases, however, data dissemination is subject to a sensitivity check.

Archiving and Disposal of Data

Paragraph (d) is a condition requiring the licensee to keep control of raw data and remote sensing products until they are disposed of. The condition has two facets to it. First of all, 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

---

[22] Bernhard Schmidt-Tedd and Max Kroymann, *Current Status and Recent Developments in German Remote-Sensing Law*, 34 J. SPACE L. 97, under Part A IV, "Conformity with UN Space Law", explain the incorporation of UN Principle XII in the *Satellitendatensicherheitsgesetz* (SatDSiG) Germany's Satellite Data Security Act in force December 1, 2007. They say, "[t]his limitation of contractual freedom in the dissemination of commercial data is the specific result of the observation of remote-sensing principles." *Id.*

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.

The archiving obligation is developed more fully in the Regulations, section 17. A licensee is required to archive raw data for at least 15 months, and is not allowed to destroy it before notifying the Minister of Foreign Affairs of the intent to destroy it. The Minister can be notified of the intended destruction any time after the data is 12 months old, and upon being notified has 3 months in which to order that the data be made available to anyone specified by the Minister, at cost.

This public interest provision is designed to give educational institutions and other entities access to data that they might not be able to afford data in the commercial market, rather than allow it to be destroyed.

Handling Raw Data

Paragraph (e), a 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.

Licensee Must Police Restrictions on Data Use

The condition in paragraph (f) 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 re-

mote 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 or by suspending the licence if the licensee violates this condition.

Fees

Paying fees (paragraph (g)) 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 important for the security of data handling are described in subsection 8(5): conditions relating to cryptography and information assurance and conditions designating system participants and the controlled activities the licensees may allow system participants to perform.

Subsections 8(6) and (7) of the Act constitute the legal authority for the Minister of Foreign Affairs to establish Customer access profiles (CAPs), the 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. CAPs are likely to 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 satel-

lite[23] are popularly called "shutter control" orders. It is noteworthy that Germany's legislation does not provide for shutter control, although the Federal Office of Economics and Export Control (BAFA), the responsible authority, may temporarily prohibit the dissemination of data.[24] In an environment where data encryption is the norm, the German law accomplishes the same practical effect as shutter control, with the advantage that the opportunity to collect data at a critical time is not lost.

The capacity for quick fine-tuning of the CAPs in Canada, allowing raw data collection but prohibiting or restricting its distribution, coupled with robust encryption of data downloaded from the satellite, should reduce or eliminate the need to invoke shutter control. Corresponding authority under United States legislation has never been used.

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. 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.

ENFORCEMENT

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

---

[23] Remote Sensing Space Systems Act, 2005 S.C., ch. 45, § 14 (Can.).

[24] SatDSiG, part 3, chapter 1, section 16. The unofficial English translation of the SatDSiG is available at 34 J. SPACE L. **. The German text is also available online at http://www.bgblportal.de/BGBL/bgbl1f/bgbl107s2590.pdf.

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 inspectors), 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.

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 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 by the Federal Court of Canada.

Penalties for Violations

Schedule 2 of the Remote Sensing Space Systems Regulations sets out 43 provisions in the Act and Regulations which, if contravened, could constitute violations under the Act. The following table illustrates typical violations and the maximum penalty that could be imposed for each.

MAXIMUM PENALTIES FOR VIOLATIONS, PER DAY

Operating when licence is suspended	$ 25,000
Disposal Plan not up to date	25,000
Allowing unauthorized person to give command to satellite	20,000
Failing to assist an inspector when requested to do so	10,000
Giving false or misleading information to an inspector	10,000
Failure to notify Minister that control of satellite has been lost	25,000
Failure to notify Minister of cryptography malfunction	25,000
Poor management of sales records	5,000
Archived data not readily retrievable	25,000
Disposal of data without proper notice	15,000
Late provision of copy of satellite launch contract	10,000
Late report of satellite launch, orbit and performance	15,000
Failure to maintain control of system	25,000
Unauthorized disclosure of raw data	20,000
Contact person does not possess required security clearance	15,000
Fee not paid when due	5,000

Offences under the Act

More serious offences may be prosecuted in the criminal courts. Some examples, with maximum penalties:

OFFENCE	INDIVIDUAL	CORPORATION
Operating satellite system without a licence	$ 50,000 and 18 mo.	$ 250,000
Transfer control without permission	$ 50,000 and 18 mo.	$ 250,000
Disobey order when licence is suspended	$ 50,000 and 18 mo.	$ 250,000
Obstructing an inspector	$ 25,000 and 6 mo.	$ 125,000
Disobey order for priority access by government	$ 25,000 and 6 mo.	$ 125,000

Injunctions

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 actually commence an unlawful operation. The Court can order them to take any measure that a licensee could be ordered to take under the Act.

PRIVACY

Although concerns about privacy were raised early and often in the legislative process, there are no provisions in the Act or Regulations dealing with privacy, and no privacy conditions

have been incorporated in the first remote sensing satellite system license.

Synthetic aperture radar (the technology under discussion for the *RADARSAT-2* satellite) does not even detect human beings as such, nor is it capable of detecting other indicia of human activity at a level considered to be a violation of individual privacy.

In this respect, Canada's constitutional protection of privacy rights has taken a different direction than the United States Fourth Amendment protection of privacy within the home and its curtilage. The *Kyllo v. United States*[25] decision in the U.S. dealt with the police use, without a search warrant, of forward looking infra-red (FLIR) sensors to detect heat emanation from a suspected marijuana grower's home. The United States Supreme Court, in a 5-4 decision authored by Justice Scalia, held that such detection revealed intimate details of human activity within the home and therefore violates the Fourth Amendment right against unreasonable searches and seizures. Justice Scalia also discussed how future technology can invade on one's right of privacy and in what he called "the long view" of the Fourth Amendment purported to extend protection against more sophisticated surveillance equipment, possibly including synthetic aperture radar of the type used in *RADARSAT-2*.

Justice Stevens, writing for the dissent in *Kyllo* stated:

> Although the Court is properly and commendably concerned about the threats to privacy that may flow from advances in the technology available to the law enforcement profession, it has unfortunately failed to heed the tried and true counsel of judicial restraint. Instead of concentrating on the rather mundane issue that is actually presented by the case before it, the Court has endeavored to craft an all-encompassing rule for the future. It would be far wiser to give legislators an unimpeded opportunity to grapple with these emerging issues rather than to shackle them with prematurely devised constitutional constraints.[26]

---

[25] Kyllo v. United States, 533 U.S. 27 (2001).

[26] *Id.* at 51.

Three years later, in the *R. v. Tessling*[27] case in Canada, which involved circumstances identical in all respects to *Kyllo*, Canada's Supreme Court concluded that infra-red imaging did not constitute an unconstitutional search without warrant, stating: "The United States Supreme Court declared the use of FLIR technology to image the outside of a house to be unconstitutional in Kyllo v. United States, 533 U.S. 27 (2001), based largely on the 'sanctity of the home' (p. 37). We do not go so far."[28]

And in contrast with the "long view" taken by Justice Scalia, the sentiment of dissenting Justice Stevens was echoed by Canada's Supreme Court, which held:

> [T]he spectre of the state placing our homes under technological surveillance raises extremely serious concerns. … such technology must be evaluated according to its *present* capability. Whatever evolution occurs in future will have to be dealt with by the courts step by step. Concerns should be addressed as they truly arise.[29]

Privacy rights are adequately protected under the search and seizure provision of Canada's Charter of Rights and Freedoms, as well as the Privacy Act, which regulates government handling of personal information, and the Personal Information Protection and Electronic Documents Act which regulates the handling of personal information in the private sector in Canada. As a result of the Canadian jurisprudence, and upon consultation with the Office of the Privacy Commissioner of Canada, it was decided that there was no need to enact additional privacy protection in the Remote Sensing Space Systems Act.

---

[27] R. v. Tessling, 2004 S.C.C. 67, [2004] 3 S.C.R. 432.
[28] *Id*. at 37.
[29] *Id*. at para. 55 (italics in original).

BELGIAN LEGAL FRAMEWORK FOR EARTH OBSERVATION ACTIVITIES

Jean-François Mayence[*]

In many respects, Belgium illustrates the involvement of small and medium size space-faring nations in everyday space activities, from basic research and development to commercial operations and exploitation of derived products. Such an involvement requires an active participation in the definition, the elaboration, the implementation, and the updating of the corresponding legal framework, be it at the international or national level.

Through its participation in the European Space Agency's (ESA) programs (which allows Belgium to use that intergovernmental organization to some extent as its own national space agency) and through bilateral cooperation with other States, the Belgian Government commits itself to bearing the risk of certain activities that are under third parties' actual control. This may appear unsatisfactory in regard to the current effort to enhance the effective control on space activities, of which earth observation is not the least hazardous area.

A country that mainly acts in outer space through the framework of an intergovernmental organization raises questions regarding the implementation of some provisions of the United Nations' space treaties. The fact that Belgium adopted, in September 2005, national space legislation does not answer all such questions because some are linked to the application of international law.

While article VI of the 1967 United Nations' Outer Space Treaty (Outer Space Treaty) imposes on State parties an international responsibility based on the control and the *continuous supervision* of the activities performed under their jurisdiction,[1]

---

[*] Head of the Legal Unit "International Relations", Belgian Federal Office for Science Policy, Brussels.

[1] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, Jan. 27, 1967, 18